行政院國家科學委員會專題研究計畫　期中進度報告

子計畫三:多階隨意網路上位置衍生的服務與應用(1/2)

計畫類別： 整合型計畫
計畫編號： NSC92-2219-E-009-012-
執行期間： 92 年 08 月 01 日至 93 年 07 月 31 日
執行單位： 國立交通大學資訊科學學系

計畫主持人： 簡榮宏

計畫參與人員： 鄭安凱、鄭旭峰、吳依萍、高玉和

報告類型： 完整報告

處理方式： 本計畫可公開查詢

中　華　民　國 93 年 5 月 27 日

行政院國家科學委員會補助專題研究計畫期中報告

※※※※※※※※※※※※※※※※※※※※※※※※※
※ ※
※ 多階層行動隨意網路之設計及實作—子計劃三： ※
※ 多階隨意網路上位置衍生的服務與應（II） ※
※ ※
※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：□個別型計畫 ☑整合型計畫
計畫編號： NSC 92－2219－E－009－012
執行期間： 92 年 8 月 1 日至 93 年 7 月 31 日

計畫主持人： 簡 榮 宏

本成果報告包括以下應繳交之附件：
□赴國外出差或研習心得報告一份
□赴大陸地區出差或研習心得報告一份
□出席國際學術會議心得報告及發表之論文各一份
□國際合作研究計畫國外研究報告書一份

執行單位： 國立交通大學 資訊科學系

中 華 民 國 93 年 5 月 27 日

行政院國家科學委員會專題研究計畫期中報告

多階層行動隨意網路之設計及實作—子計劃三：多階隨意網路上位置衍生的服務與應（II）

Location-Base Services and Applications for Multi-tier Ad Hoc Networks

計畫編號：NSC 92-2219-E-009-012
執行期限：92 年 8 月 1 日至 93 年 7 月 31 日

主持人：簡榮宏　　國立交通大學資訊科學系
計畫參與人員：鄭安凱、鄭旭峰、吳依萍、高玉和
國立交通大學資訊科學系

中文摘要

近年來由於無線區域網路的普及，影響人們在無線區域網路下的使用習性，不論是在室外或室內均希望能有位置相關 (location-based)的服務。在本計畫中，首先對細胞格為主的定位方法(cell-based location determination method)再加以分析及改進，並整合室內及室外不同的定位技術，開發位置閘道器(Location Gateway)，讓使用者不論在何種環境下，都能有無接縫換手(seamless handoff)的定位系統可以使用。

關鍵詞：無線區域網路、位置相關、細胞格為主的定位、位置閘道器

Abstract

With the development of Wireless Local Area Networks (WLANs), people are interested in developing the location-based services for WLAN users. The core technology of location-based services is the positioning system. In this project, we analyze and improve the cell-based positioning method. Then, we implement a location gateway that integrates signal fingerprinting and global positioning system. In this integrated system, mobile users can switch their positioning systems from one to another transparently.

Keywords: Wireless local area networks、Location-based、Cell-based、Location gateway

目錄

一、前言

由於無線區域網路技術的進步及廠商大量生產，而導致相關的產品價格下降，除了機場、學校、咖啡店、速食店等公共場能採用無線區域網路來節省成本外，也使得個人及家庭用戶的使用者也轉向採用無線網路，這樣的轉變不僅如此，更延伸至其他方面的設備，如筆記型電腦、PDA、手機，甚至是資訊家電等都具備無線網路傳輸功能。這樣眾多的無線設備讓使用者可以不受限制的在任何場所，任何地點，任何時間都能上網獲取所需的資訊，如此方便使用的特性也衍生出許多的應用，如旅遊資訊的導覽[1]、行車導航[2]及路況資訊的提供、緊急救援服務[3]等等，而這麼多應用服務(application services)的開發其背後均是憑藉著位置資訊來完成該服務，然而所提供的位置資訊是否正確，精確度是否適合，都會影響著應用程式的服務品質及其正確性。因此，位置資訊的研究便成了開發以位置資訊為導向(Location-based Services)的應用程式的重要技術。

位置資訊的研究包含有定位技術、位置資訊的隱私性問題、地理資訊的呈現問題等，但其中具有決定性關鍵因素的技術為定位技術，這是因為位置資訊的正確性是在開發以位置資訊為導向的應用程式核心技術的必備要件，因此，這也成為當前在無線網的應用方面的研究重點項目之一。

目前定位的技術已有不少方法被提出或實作出來，概分為以下幾類(1)以網路架構為主的解決方法：包含(a)訊號到達基地台的夾角(Angle of Arrival, AOA)[4,5]、(b)訊號到達基地台的時間差(Time Difference of Arrival, TDOA)[4,5] 、(c)混合(1)及(2)的方法(AOA+TDOA)[4,5]等，此類方法需在網路端加入額外的設備來達成，花費較高，而定位精確度中等；(2)以手機架構為主的解決方法：包含(a)全球衛星定位系統(Global Positioning System, GPS)[6,7]、(b)輔助全球衛星定位系統(Assisted-GPS)[8,9]等，此方法的定位需在使用者端加入全球衛星定位系統接收器，且第一次定位的時間較長，但定位的精確度較高。(3)混合第一和第二類型的強化監視式時間差(Enhanced-Observed Time Difference, EOTD)[5](4)以軟體方式的解決方法–強化式細胞識別(Enhance Cell ID, ECID)[5]，此方法的定位精確度介於第一及第二種方法，但花費之成本較二者低。

上述之方法為常見的室外定位技術，然而在室內因為建築物牆壁及地板的阻隔影響，造成上述定位方法獲得的位置資料有誤差。因此，對於室內定位技術[10,11]方面，另外發展出以下幾種方法(1)利用已存在的網路架構：例如利用無線網路來定位(2)利用額外的網路架構：例如建置紅外線網路系統來偵測使用者位置。一般來說，目前較常採用第一種室內的定位方法，原因是無線網路是現存的網路系統，不需額外的建置費用。相對的，採用第二種室內定位的方法因為要部署一個特別的定位用網路系統花費很高。

然而如可在眾多的定位技術中整合一個適用於各種環境的定位系統也是一個值得探討的問題，為了能使各種定位技術及位置資訊為導向應用程式的開發能具彈性架構及模組化的功能，發展位置閘道器(Location Gateway)成為一可行的方法，位置閘道器是用來負責接收位置為導向的應用程式的位置要求，由其內的決策模組依網路系統及使用裝置來決定啟動何種定位技術，並將計算後之位置資訊回應至應用程式。位置閘道器的開發使得定位技術與定位應用區分開來，亦即未來可不必等到各地系統都上線後才能推出對應服務，而且當有新的定位技術或新的定位應用開發出來後，只需略微修改位置閘道器的決策模組就可以很快的將兩者整合在一起。

本計畫已在第一年完成室內及室外的定位技術的開發，因此，在本年度的計畫中，我們除了改進所開發的定位技術，使其能更適合於現有的無線網路環境下能有較好的定位精確度，也針不同定位系統的整合開發出位置閘道器，讓使用者不必理會現在的定位系統為何？現在的位置為何？就能完成定位，而定位技術與位置資訊為導向應用的研發也能獨立開發不會互相干擾或影響。

二、研究目的

定位技術的重要性已成為無線網路研究的重要項目之一，以目前定位技術的發展狀況，使用者在不同的環境（最明顯的是室內及室外的差別），所能使用的定位技術也有所不同，這是由於定位技術的適用範圍及其精確度的影響所致，因此，本計畫將針對上一年度所開發的定位技術－細胞格為主的定位方法(cell-based positioning method)加以分析與改進，探討基地台故障時定位系統的強壯性(robustness)，並設計訊框(beacon frame)格式讓使用者的裝置能根據所接收到的訊框資料配合簡單的運算即可獲得自己的位置資訊，以期能將其實際應至現有的無線網路環境下。

在完成定位技術的改進後，另一個重點則為位置閘道器(location gateway)的開發，位置閘道器能整合各項定位技術，讓使用者在任何地方均不必理會現在所使用的定位系統為何，而定位技術與位置資訊為導向應用的研發也能獨立開發不干擾或影響。在本計畫中我們將整合室內的訊號特徵(signal fingerprinting)定位技術及室外的全球衛星定位技術(GPS)，實際開發出位置閘道器及其所需的位置決定模組(location decision module)，如此不僅可驗證理論的可行性，並透過此一實做發展出一個同時符合室內及室外環境的整合型定位系統。另外，由於使用者在室內及室外的環境而採用不同的定位技術，而不同定位技術的切換是否會造成位置資訊的誤差、延遲(delay)或中斷都是需要研究的課題，我們亦將對此問題加以改進，能開發出整合型無接縫換手(seamless handoff)的定位技術。

三、文獻探討

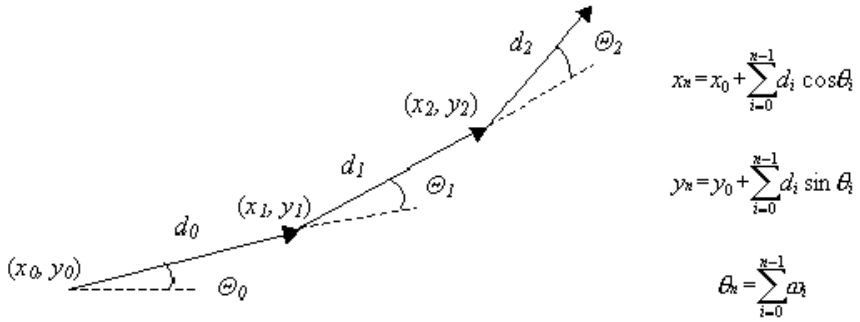
各種已經開發的定位技術如下所述：

1. 以網路架構為主的定位技術：在網路端的中央伺服器負責收集手機的訊號並決定（計算）出使用者的位置。
   - 訊號到達基地台的夾角(Angle of Arrival, AOA)[4,5]：基地台需額外建置一個能辨別訊號送至基地台時的角度的天線，利用使用者與其所有相臨的基地台的訊號夾角，再利用三角測量來獲得使用者的位置資訊。
   - 訊號到達基地台的時間差(Time Difference of Arrival, TDOA)[4,5]：基地台需額外建置一個設備，它能辨別訊號送至基地台時的時間差，利用使用者與其所有相臨的基地台的訊號時間差，來獲得使用者的位置資訊。
   - 混合(1)及(2)的方法(AOA+TDOA)[4,5]
2. 以手機架構為主的定位技術：手機負責接收從網路送出的訊號，並決定（計算）自己的位置。
   - 全球衛星定位系統(Global Positioning System, GPS)[6,7]：利用環繞地球的 24 顆衛星，將衛星精確的速度、高度、經度、緯度傳送到使用者的全球衛星定位系統接收器，然後再由手機自行決定（計算）自己的位置。
   - 輔助全球衛星定位系統(Assisted-GPS)[8,9]：方法類似全球衛星定位系統，但在網路端加入一個位置修正伺服器。因為衛星傳送的資訊會因為地表空氣的折射干擾而產生誤差，故透過此位置修正伺服器將所決定（計算）出的位置資訊加以修正，以獲得較精確的位置資訊，並節省手機的電力消耗。
3. 以軟體方式的解決方法–強化式細胞識別(Enhance Cell ID, ECID)[5]，利用基地台發出個別的識別記號(Cell ID)，根據使用者接收到不同的識別記號群組來決定其所在的位置，例如以細胞格為主的定位方法(cell-based position method)。此方法會涉及覆蓋範圍的問題探討(coverage area problem)其整合計算幾何學與圖形理論技術及其相關

的演算法來計算[12]，也有採用方位(exposure)配合最短路徑的演算法來解決此問題[13]，亦有利用凸面(convex)區域化簡的方法[14]及以無線電波強度的方法[15]。另外，覆蓋範圍的大小亦會影響基地台發射的功率及其耗電量，故決定覆蓋範圍的大小對功率調整控制的機制[16,17,18]也要要加以考慮。

4. 航位推算(Dead Reckoning System, DR)定位技術：

航位推算(DR)是非常早期的定位技術，被用在航海和汽車導航上，它的基本觀念是用感測器去測量移動物體的方向和距離，整合移動物體的方向和距離再加上起始點的位置資訊，便可計算出移動物體目前的位置和方向（如圖一所示）。



圖一：航位推算定位技術

其中(x_0,y_0)是在時間點 t_0 的起始點，d_i 是移動的距離，θ_i 是移動方向，ω_i 則是角速度。DR 雖然是一種自足式的定位方式（即不用憑藉其它系統的協助就能自行作位置估測），但 DR 也有其缺點，就是它的精確度會隨著時間的增加而持續下降，這是因為每次位置估算的誤差累積所造成的，因此，單靠此定位方式仍是不足夠的。

5. GPS/DR 定位系統[19, 20]：

因為 GPS 的訊號在某些有遮蔽的地點無法收到，而 DR 系統會隨著時間增長而加大的誤差。因此，將此兩系統作整合，便可將兩種定位技術截長補短，成為一個更佳的定位方式。它的基本觀念就是以 GPS 和 DR 的定位方式為基礎，使用卡門濾波(Kalman filtering)的技術來做訊號的融合。在這樣的整合系統下，GPS 來幫助 DR 控制它的誤差在一定範圍內，而 DR 則作為當 GPS 訊號被遮蔽時的主要定位方式。

6. 室內定位技術方面有兩種常用的技術(1)利用已存在的網路架構：例如利用無線網路來定位的 RARDAR[21]系統(2)利用額外的網路架構:例如建置紅外線網路系統來偵測使用者位置的 Active Badge system[22]。

四、研究方法

本計畫要在多階隨意網路上發展位置衍生的服務與應用，基本架構如圖二所示，分為四個主要的功能區塊，(1)定位技術(Location Determination Technologies) (2)位置閘道器 (Location Gateway) (3) 位置資訊 (Location Provisioning)(4) 服務應用程式 (Applications)，各區塊內基本功能概述如下：

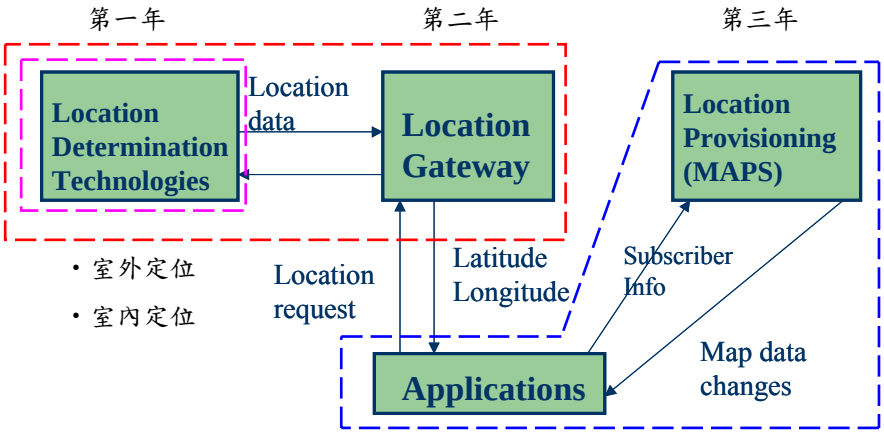
(1)定位技術(Location Determination Technologies)：包含基地台(發射器)之位置資訊之資料庫及針對各種網路環境及狀況計算其位置資訊的模組。

(2)位置閘道器(Location Gateway)：負責接收位置為導向的應用程式之位置要求，並發展一決策模組依網路系統及使用裝置來決定啟動適當的定位技術，並將計算後之位置資訊回應至應用程式。

(3)位置資訊(Location Provisioning)：提供位置為導向的應用程式所須之位置資訊，如地圖、座標、相對位置或經緯度等資訊。

(4)服務應用程式(Applications)：在各行動裝置上開發位置為導向的服務應用程式，向位置閘道器提出位置資訊之需求，取得後再依位置資訊向地理資訊模組取得對應的地理資訊。

此架構運作方式是由服務應用程式向位置閘道器提出位置資訊的要求(location request)，而位置閘道器便依此要求，來尋求欲定位物件可用的定位技術(Location Determination Technologies)並向其要求位置資訊，待該定位系統計算出位置資訊(location data)即傳回給位置閘道器，此時位置閘道器再將位置資訊(經緯度資訊 latitude longitude)回應給所要求之應用程式。當應用程式獲得位置資訊後便能依此再與地圖資訊(map data)或其他提供之位置資訊(Location Provisioning)結合來達成更人性化、個人化的位置導向的服務與應用。其中應用程式透過位置閘道器，獲取欲定位物件的位置，可不必知道該物件目前所在的網路及其是採用何種定位的機制，只須對位置閘道器發出要求即可，且定位技術的修改及增加並不影響原有的應用程式。本年度計劃（第二年）主要可分為兩部分，一是針對所開發的定位方法的加以改進，另一是利用位置閘道器發展出整合室內及室外的無接縫換手(seamless handoff)定位系統。分述如下：

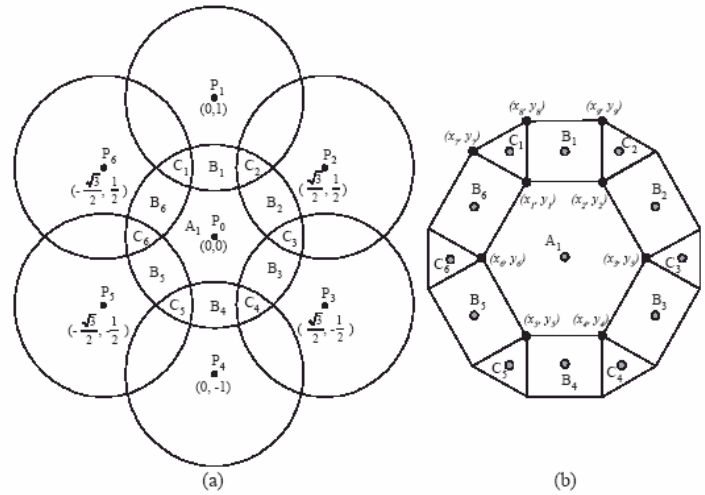


圖二：本計畫基本架構圖

1. 定位技術分析及改進：

(1) 對於上一年度所開發的以細胞格為主的定位方法(cell-based positioning method)，我們分析其在基地台發生故障時的定位精確度分析，經實驗結果顯示，此定位方法在基地台故障時仍保有不錯的定位精確度。

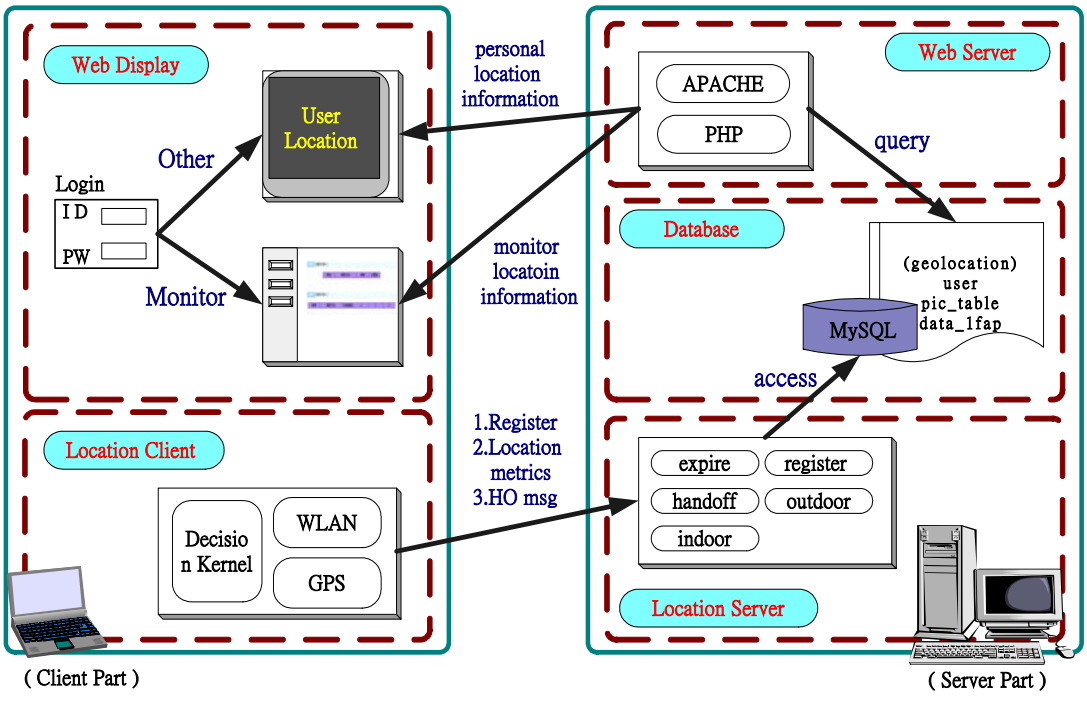
(2) 改進以細胞格為主的定位方法(cell-based positioning method)，將訊號重疊的區域與面積的質心相結合，將原本的定位精確度以訊號重疊區域的表示方式，改由該區域的質心來表示(如圖三所示)，並探討精確度的變化及系統的效能。另外，亦將原本集中式的定位方式（位置資訊傳至位置伺服器處理）經由我們設計的訊框格式(beacon frame)夾帶位置訊息的方式，使得每個使用者可以利用本身的裝置，藉由簡單的數學運算即可自行定位，完成分散式的定位技術。



圖三：重疊區域(a)轉換成質心(b)的表示方式

2. 位置閘道器的開發：

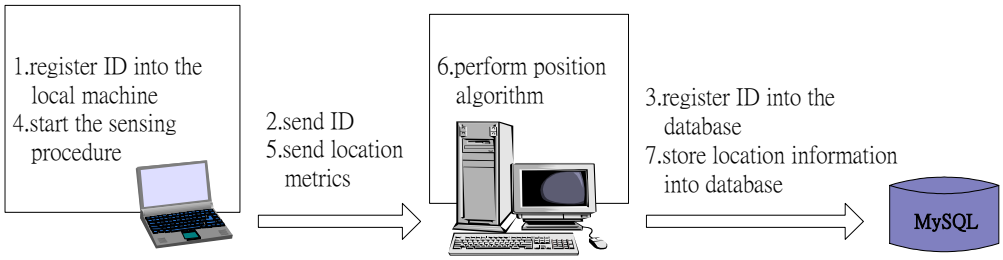
我們提出一個整合性的架構，可以整合不同性質的定位方法，在此我們僅以兩種較常用的定位方式來實做整合，一個是室外的定位技術(GPS)；另一個則是室內的訊號特徵(signal fingerprinting)的定位技術。另外，我們也提供一個無接縫的位置換手模式，使得當使用者所在的位置(室內或室外)改變時，系統能作適當的轉換並讓使用者不會感覺有任何的異狀，且不因環境的改變而使其定位應用程式中斷服務。系統整體架構如圖四所示。



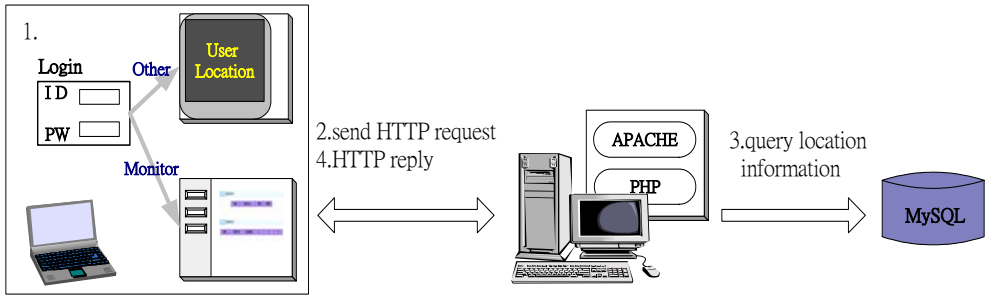
圖四：整合室內及室外的無接縫換手(seamless handoff)定位系統之架構圖。

此系統是一個主從式(client-server)的架構，每個部分由數個模組組成，在以客戶端(client)的主要工作：(1)進行環境的偵測及收集有關的位置訊息，並將此位置訊息送至伺服端(server)；(2)將使用者的位置呈現在網頁上。而伺服端(server)的主要工作也有兩項：(1)將客戶端送來的位置訊息配合定位的技術來估計使用者目前所在的位置，並將此位置資訊儲存在資料庫中；(2)查詢資料庫來取得使用者的位置資料，並將其回傳給使用者，讓使用者端能以網頁的方呈位置資訊。以下分別說明各項細節：

(1)操作流程（如圖五）：要使用本系統，首先要啟動客戶端背景程式，向伺服端註冊(如步驟 1-3)，並讓此背景程式去收集位置訊息後送到伺服端作處理(如步驟 4-6)，得到位置資訊再存放在資料庫(如步驟 7)。完成上述動作後，要將使用者位置資訊呈現出來，則要透過網頁來顯示，其操作流程如圖六所示。

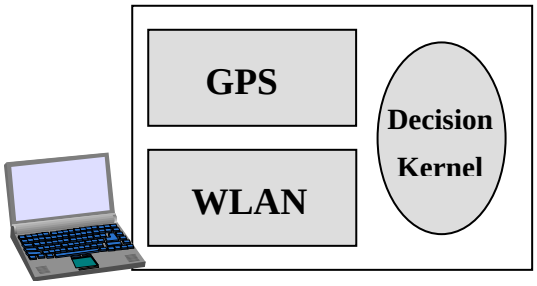


圖五：系統操作流程



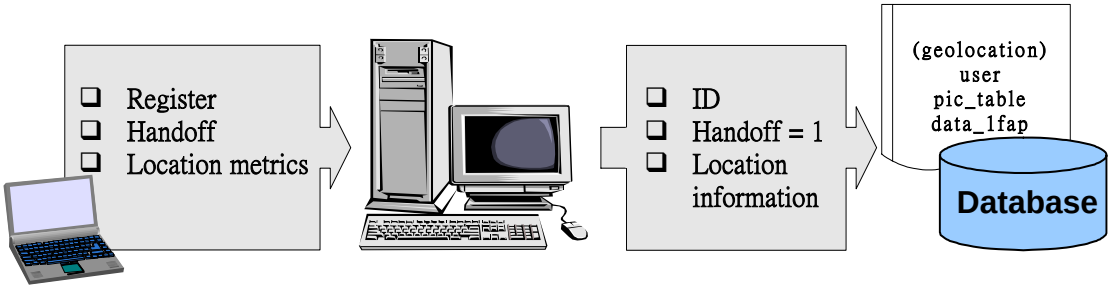
圖六：位置資訊的呈現流程

(2)客戶端背景程式（如圖七）：此程式是在 Window XP 作業系統的 Windows DDK 環境下，以 C 語言來實作，程式的主要功能是偵測環境特性並產生位置量測訊息，這些訊息當使用者處在室內環境時是收集所有 AP 的訊號強度；在室外時則是 GPS 接收器所計算的位置座標（經度、緯度及高度）。另外，它還有一個決策模式能夠分辨現在使用者所處的環境是在室內或是室外，及決定要送給伺服器哪種位置訊息，最後尚須判斷是否需要作換手(handoff)的動作。



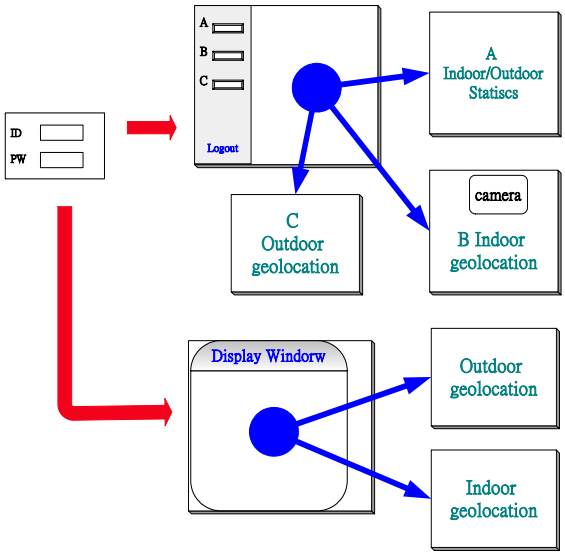
圖七：客戶端架構

(3)伺服端程式：伺服端程式是在 Red Hat9.0 的平台上，用 Java 的語言寫成，其功能如圖八所示，它會從客戶端接收一些訊息，完成處理後再存放至資料庫中，伺服端程式如果收到的是室內傳來的訊息，則會執行室內的定位演算法，而得到使用者在室內的估計位置；如果收到室外的訊息，則會從中取得使用者的經緯度座標，再將這些資訊存放在資料庫內。



圖八：伺服端架構

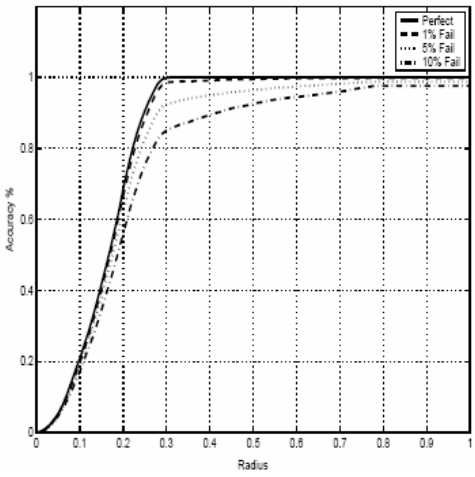
4.位置呈現系統（如圖九）：利用網頁的方式呈現，使用者會依不同的權限而得到不同的網頁呈現，管理者的權限高可進入監控畫面，並可看到本系統上的所有使用者的位置資訊，而一般的使用者權限低僅能看到個人位置資訊畫面，此畫面會根據使用者的位置改變而動態的更改來呈現出使用者正確的位置。



圖九：位置資訊呈現方式流程

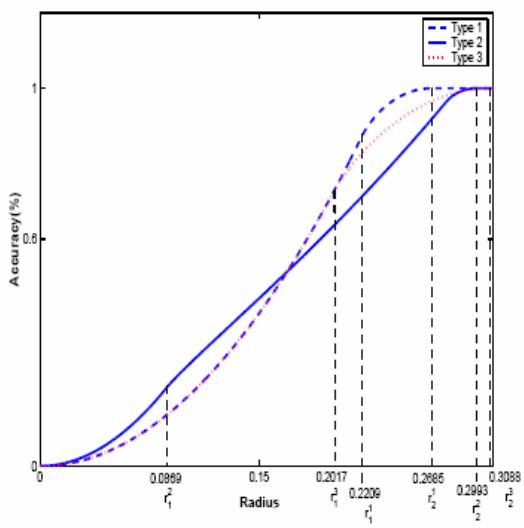
五、結果與討論(含結論與建議)

本年度本計畫完成了細胞格為主的定位方法(cell-based location determination method) 之分析，其在基地台發生故障時的定位精確度如圖十所示，可看出有 10%的基地台故障狀況下，在 0.3 單位長的誤差範圍內仍可達到 85%的定位精確度，顯示我們所開發的定位技術具有強壯(robustness) 的特性。

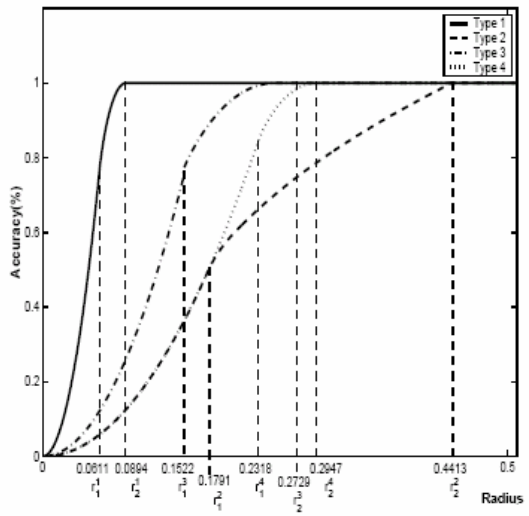


圖十：基地台故障與定位精確度之關係

我們設計的訊號格式(beacon frame)夾帶位置訊息的方式與質心的表示方式，改進了細胞格為主的定位方法，使得每個使用者可以利用本身的裝置，藉由簡單的數學運算即可自行定位，系統的定位精確度如圖十一、十二所示，在六角形(格狀)網路結構下，在誤差為 0.3088 (0.4413) 的單位長度內的系統定位精確度可達 100%。

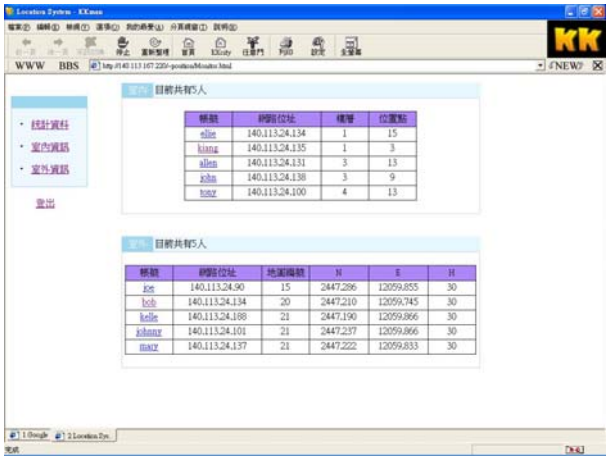


圖十一：在六角形網路結構下之系統定位精確度



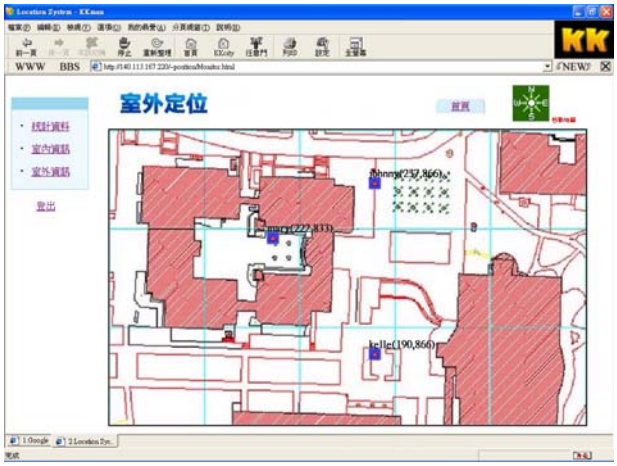
圖十二：在格狀網路結構下之系統定位精確度

另外，我們實際開發完成整合室外的GPS 定位技術與室內的訊號特徵(signal fingerprinting)定位技術的系統，包含位置閘道器及其所需的定位技術決策模組的開發，此系統具有定位技術無接縫換手(seamless handoff)的功能，實作之系統操作展示畫面如圖十三～十五所示。



圖十三：系統主畫面

圖十四：室內位置資訊的呈現



圖十五：室外位置資訊的呈現

六、第三年的預定研究項目：

第三年預定研究項目為多階無線隨意行動網路具位置知覺的服務與應用，其主要探討內容可分為下列三部分：

(1)建置一地理資訊與服務資訊系統包含地圖、地圖、座標、相對位置或經緯度等資訊提供系統。

(2)整合定位系統、位置閘道器、地理資訊系統及相關的資訊，開發一具位置知覺的服務與應用，我們將分兩類來研究：第一類為位置追踪服務－我們將依移動之軌跡資訊來發展提供服務，例如：人員的搜尋、設備的管理及自己位置查詢(where am I ?)…等的服務應用程式；第二類為位置資訊應用－我們將利用位置的資訊發展出具位置知覺的應用程式。

(3)繼續改進定位的技術，探討在細胞格為主的定位方法(cell-based positioning method)下，基地台具有多階訊號強度 (multiple power-level)的定位技術。

七、參考文獻

[1] N. Davies, K. Cheverst, K. Mitchell, and A. Efrat, “Using and determining location in a context-sensitive tour guide”, *Computer*, vol. 34(8), Aug. 2001, pp. 35-41.

[2] T.S. Rappaport, J.H. Reed, and B.D. Woerner, “Position location using wireless communications on highways of the future,” *IEEE Communications Magazine*, pp. 33-41, Oct. 1996.

[3] J. M. Zagami, S. A. Parl, J. J. Bussgang, and K. D. Melillo, “Providing universal location services using a wireless E911 location network”, *IEEE Communications Magazine*, vol.36(4), Apr. 1998, pp. 66-71.

[4] C. Drane, M. Macnaughtan, and C. Scott, “Positioning GSM telephones,” *IEEE Communications Magazine*, vol. 36(4) , Apr. 1998, pp.46-54.

[5] J. Bensche, J. Cooke, E. Job, T. Luke, J. Kvaal, and N. Swatland, “Investing in The Wireless Location Services Market,” *Lehman Brothers Report*, Sep. 2000.

[6] E. G. Masters, C. Rizos, and B. Hirsch, “GPS...more than a real world digitizer”, *IEEE Position Location and Navigation Symposium*, 1994, pp. 381-387.

[7] K. Chadha, “The Global Positioning System: Challenges in Bringing GPS to Mainstream Consumers”, Proc. of IEEE International Conf. on Solid-State Circuits, 1998, pp. 26-28.

[8] G.M. Djuknic, and R.E. Richton, “Geolocation and assisted GPS”, *Computer*, vol. 34(2), Feb. 2001, pp. 123-125.

[9] E. Kotsakis, A. Caignault, W. Woehler, and M. Ketselidis “Integrating Differential GPS data into an Embedded GIS and its Application to Infomobility and Navigation”, *7th EC-GI & GIS WORKSHOP EGII -Managing the Mosaic Potsdam*, Germany, June 13-15, 2001.

[10]M. Wallbaum, ”Wheremops: An Indoor Geolocation System,” *Proc. of 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* , vol. 4, 2002, p.1967-1971.

[11]K. Pahlavan, and X. Li, ”Indoor Geolocation Science and Technology,” *IEEE Communications Magazine*, vol. 40, Feb. 2002, p.112-118.

[12] S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, “Coverage problems in wireless ad-hoc sensor networks”, *Proc. of IEEE INFOCOM*, vol. 3, 2001, pp. 1380-1387.

[13] S. Meguerdichian , F. Koushanfar , G. Qu , and M. Potkonjak “Exposure in wireless Ad-Hoc sensor networks”, *Proc. of Seventh Annual International Conf. on Mobile Computing and Networking*, July 2001.

[14] L. Doherty et al., “Convex Position Estimation in Wireless Sensor Networks,” Proc. Infocom 2001, IEEE CS Press, Los Alamitos, Calif. 2001.
[15] N. Bulusu, J. Heidemann, D. Estrin, “GPS-less low-cost outdoor localization for very small devices,” *IEEE Personal Communications*, Oct. 2000, pp. 28-34.
[16] S.-L. Wu, Y.-C. Tseng, and J.-P. Sheu, “Intelligent Medium Access for Mobile Ad Hoc Networks with Busy Tones and Power Control”, *Proc. of Eight International Conference on Computer Communications and Networks*, 1999, pp. 71-76.
[17] C.-F. Hunag, Y.-C. Tseng, S.-L. Wu, and J.-P. Sheu, “Increasing the Throughput of Multihop Packet Radio Networks with Power Adjustment”, *Proc. of 10th International Conf. on Computer Communications and Networks*, 2001, pp. 220-225.
[18] Y.-C. Tseng, S.-L. Wu, C.-Y. Lin, and J.-P. Sheu, “A Multi-Channel MAC Protocol with Power Control for Multi-Hop Mobile Ad Hoc Networks”, *Proc. of Distributed Computing Systems Workshop*, 2001, pp. 419-424.
[19] Q. Wu, Z. Gao, Y. Wang, “Study on GPS/DR/MM integrated navigation system for vehicle based on DSP”, *IEEE International Conference on Communications, Circuits and Systems and West Sino Expositions*, vol. 2 , July 2002.
[20] R. Jirawimut, P. Ptasinski, V. Garaj, F. Cecelja, and W. Balachandran, ” A method for dead reckoning parameter correction in pedestrian navigation system”, *IEEE Transactions on Instrumentation and Measurement*, vol. 52, pp. 209-215, Feb. 2003.
[21]P. Bahl, and V. Padmanabhan, ”RADAR: An In-Building RF Based User Location and Tracking System,” *Proc. of IEEE INFOCOM*, vol. 2, Mar. 2000, p.775-784.
[22]R. Want, A. Hopper, V. Falcao, and J. Gibbons, ”The Active Badge Location System,” *ACM Transactions on Information Systems*, vol. 40, January 1992, p.91-102.

本年度已發表或審核中之論文：

附件一

Rong-Hong Jan, Yong-Sheng He, and Chia-Tai Tsai, "An Implementation of IEEE 802.1x and RADIUS for IPv6 Networks", 10th mobile computing workshop, pp. 259-266, 2004. (Excellent paper award)

附件二

Shih-Chang Huang and Rong-Hong Jan, "Energy-Aware, Load Balanced Routing Schemes for Sensor Networks", 10th International Conference of Parallel And Distributed Systems, Newport Beach, CA, 2004.

附件三

Rong-Hong Jan, Hung-Chi Chu, and Yi-Fang Lee, “Improving the Accuracy of Cell-Based Positioning for Wireless Networks”, submitted to Computer Networks (minor revision).

附件一

An Implementation of IEEE 802.1x and RADIUS for IPv6 Networks*

Rong-Hong Jan†, Yong-Sheng He, and Chia-Tai Tsai
Department of Computer and Information Science
National Chiao Tung University
Hsinchu, 30050, Taiwan

Abstract

Security and authentication are the most important issues in wireless networks. In recent years, IEEE 802.1x, proposed by IEEE, provides a proper authentication architecture. It has been used in wireless local area networks widely. In IEEE 802.1x architecture, authentication server is responsible to authenticate users and manage users' information. Authenticator is responsible to transfer the authentication messages between users and authentication server. In general, authenticator and authentication server use the RADIUS protocol to communicate with each other. However, the existing softwares and devices that implement IEEE 802.1x and RADIUS protocol work over IPv4 networks. Up to now, we did not find authentication systems based on IEEE 802.1x and RADIUS protocol run over IPv6 networks. In this paper, we present an implementation of IPv6 authentication system based on IEEE 802.1x and RADIUS protocol to provide authentication to wireless LAN users. A prototype is presented to demonstrate that our approaches are feasible.

Keywords: Wireless LAN, IEEE 802.1x, IPv6, RADIUS, EAP.

1 Introduction

In recent years, wireless networks grow quickly and become more popular. It is desired that mobile users are able to get news, send email, access Internet content or any other information from Internet anywhere and anytime. A lot of places have constructed IEEE 802.11b wireless networks which can provide users to connect to Internet. Because it doesn't have any restrict in the default setting of access point, anyone can connect to backbone network and access Internet resources via access point. Thus, how to manage access point in effect and how to avoid invalid users using the access point arbitrarily are the most important issues in wireless LANs.

In general, there are several methods, such as access control list and wired equivalent privacy, to control users to access wireless LANs. Among these methods, access control list is the simplest. In the access control list, network administrators can configure MAC address list to allow specific MAC addresses to pass through or to deny specific MAC addresses to access. Although every NIC has its unique MAC address, users can modify it easily. Hence, access control list is insecure. Another method is using authentication system, such as Wired Equivalent Privacy (WEP) [1]. WEP authenticates users using shared-key between the access point and mobile stations. Thus, how to manage shared-key in effect and how to avoid using duplicate shared-key are the main problems. However, there are a lot of shortcomings for WEP method to authenticate mobile users. Therefore, a new architecture, known as IEEE 802.1x [2], which is based on IETF's EAP method [3], has been proposed.

The advantage of using IEEE 802.1x is that the authentication exchange is logically carried out between the user and the authentication server. The actual authentication mechanism is implemented by the authentication server. Access point just knows how to communicate with an authentication server, and then encapsulates user's authentication messages and forwards the packet to an authentication server. The authentication server supplies several authentication mechanisms, such as Extensible Authentication Protocol (EAP)-MD5 [3], EAP-Transport Layer Security (TLS) [4] and so on. Thus, network administrator can manage access point easily, as well as centralized the authentication of users.

Nowadays, many vendors, such as CISCO, Lucent, INTEREPOCH, have produced access points that support IEEE 802.1x and RADIUS protocol. Besides, there are many different authentication servers that implement RADIUS protocol, like Microsoft IAS, FreeRADIUS [7]. But,

[1]This work was supported in part by the Lee and MTI Center for Networking Research, NCTU, Taiwan and the Ministry of Education and National Science Council, Taiwan, ROC, under grants 89-E-FA04-1-4 and NSC 92-2219-E-009-012, respectively.

[2]Corresponding Author. Fax: 886-3-5721490; e-mail: rhjan@cis.nctu.edu.tw

all of them run over IPv4 networks. Up to now, we do not find IPv6 authentication systems which are based on IEEE 802.1x and RADIUS protocol. In this paper, we present two approaches to providing authentication to mobile stations for the IPv6 [8] environment as follows.

1. IPv4/IPv6 RADIUS gateway approach:

   Gateway approach is just an approach used in the transition stage, not a final solution. But, using gateway is a solution if there are no IPv6-RADIUS server. In this approach, we use a gateway to communicate with the access point and the IPv4-RADIUS server. This gateway, which supports IPv4 protocol and IPv6 protocol, is responsible for transferring authentication data between access points in IPv6 networks and the IPv4-RADIUS server. The architecture is shown in Figure 1.

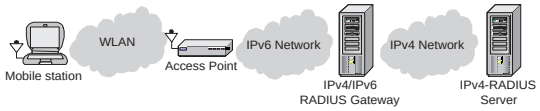


Figure 1. IPv4/IPv6 RADIUS gateway architecture

2. IPv6-RADIUS server approach:

   In this approach, we have an access point that supports IPv6 RADIUS [9] and can communicate with the RADIUS server in IPv6 networks. Besides, we also have an RADIUS server that supports IPv6 RADIUS and can run over IPv6 networks. We named this RADIUS server as IPv6-RADIUS server. The architecture is shown in Figure 2.

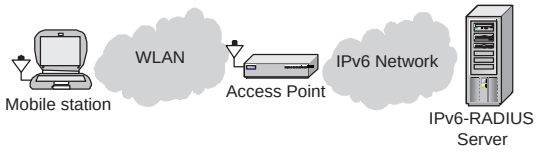


Figure 2. IPv6-RADIUS server architecture

In this paper, we implement two approaches for constructing an IPv6 authentication system based on IEEE 802.1x and RADIUS protocol. At first, we modify an open-source software, HostAP [10], which can simulate access point, to support IPv6 RADIUS protocol and communicate with IPv6-RADIUS server or IPv4/IPv6 RADIUS gateway. Then, we develop an IPv4/IPv6 RADIUS gateway which plays a protocol translator role in this environment. Finally, we modify an open-source software, FreeRADIUS, a well known authentication, authorize, accounting (AAA) server, to run over IPv6 networks properly.

In this paper, there are two mobile stations, one uses Linux as the platform, and the other uses Microsoft Windows 2000 as the platform. We use EAP-TLS or EAP-MD5 authentication mechanism to test our access point, IPv4/IPv6 RADIUS gateway, and IPv6-RADIUS server. After authenticating, we use ping and HTTP to evaluate if mobile stations can access Internet.

In section 2, we will describe our system architecture. In section 3, we illustrate our experiment environment. Finally, a conclusion is given in Section 4.

2 System Architecture

2.1 Overview

The system architecture is shown in Figure 3. There are two cases for authentication process. One includes mobile stations, access points, gateway, and an IPv4-RADIUS server. In this case, we assume that access point supports IEEE 802.1x and IPv6 RADIUS and there are no IPv6-RADIUS servers. So, we use a gateway to connect access point in IPv6 networks with IPv4-RADIUS server, and deal with IPv6 RADIUS packets from access points or IPv4 RADIUS packet from RADIUS server. The other part includes mobile stations, access points, and an IPv6-RADIUS server. In this case, we implement an IPv6-RADIUS server and access points which support IPv6 RADIUS. Therefore, they can communicate with each other.

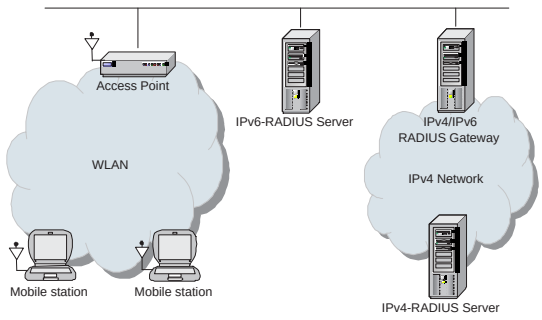


Figure 3. System architecture

2.2 Access Point

HostAP, written by Malinen [10], is used to simulate an access point. It is a Linux driver for wireless LAN cards based on Intersil's Prism2/2.5/3 chipsets. This driver supports a so called Host AP mode which deals with IEEE 802.11 management functions in the host and acts as an access point. HostAP driver also includes PAE functionality in the kernel driver. It is a relatively simple mechanism for denying normal frames which are coming from

an unauthorized port. In general, HostAP can be divided into two parts. One part is driver and modules, and the other part is *hostapd*, a user space daemon, that implement IEEE 802.1x Authenticator functionality. By executing *hostapd* daemon, system is capable of processing IEEE 802.1x frames and RADIUS packets. In conclusion, the driver needs to be compiled for user space management functionality and *hostapd* needs to be executed. Now, system acts as an access point and can provide IEEE 802.1x authentications.

In addition, HostAP also supports wireless distribution system (WDS), access control list (ACL) for stations, WEP, and so on. These functions can be used by executing system commands, such as commands provided by wireless-tools software and utilities which are provided by HostAP itself.

The basic operation of *hostapd* is shown in Figure 4.

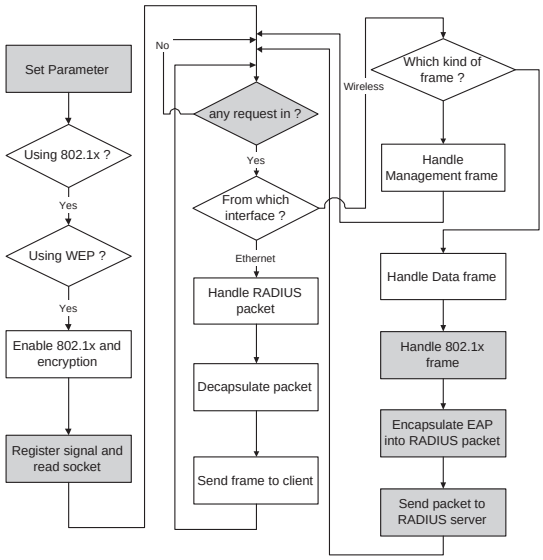


Figure 4. The process of *hostapd*

Besides supporting IEEE 802.1x and IPv4 RADIUS, we hope that access point also supports IPv6 RADIUS. In other words, we let access point support not only IPv4 RADIUS but also IPv6 RADIUS. We also let it can communicate with IPv6-RADIUS server. According to RFC 3162, IPv6 RADIUS adds some attributes, including NAS-IPv6-Address, Framed-IPv6-Prefix, Framed-IPv6-Route and so forth. Therefore, there are two major modifications made to HostAP, one is adding IPv6 attributes, and the other is modifying functions to support IPv6. Gray block diagrams in Figure 4 are sections we have modified. The following sections illustrates where we modify and why we modify it.

1. hostapd.c

   This is the main program that provides IEEE 802.1x/RADIUS functionality. First, we have to add IPv6 address structure and IPv6 socket. Besides, we should use some functions to deal with IPv6 address, such inet_ntop and inet_pton.

2. hostapd.h

   This file includes the main structure that to be used in this program. We add some parameters about IPv6 into this structure.

3. ieee802_1x.c

   This file includes a lot of functions about the process of IEEE 802.1x frames. We can understand how it deals with frames, parse frames, etc. The most important function here is to encapsulate EAP message and RADIUS attributes into RADIUS packet, and decapsulate RADIUS packet. Thus, we can encapsulate IPv6 attributes by modifying these functions.

4. Radius.c and Radius.h

   These two files include RADIUS attributes structure. We add attributes about IPv6 RADIUS here. And there are some functions that process IP address, we modify it to support IPv6 address format.

The capability of new access point is summarized as follows. The new AP supports IPv6 RADIUS attributes and encapsulates NAS-IPv6-Address attribute into RADIUS packet. Besides communicating with IPv4 RADIUS server, this new access point can also communicate with IPv6-RADIUS server or IPv4/IPv6 RADIUS Gateway.

2.3 IPv4/IPv6 RADIUS Gateway

The IPv4/IPv6 RADIUS gateway acts as a proxy server. It receives RADIUS packets from access points in IPv6 networks or IPv4-RADIUS server, processes them, and then sends to the other side. Using gateway is a good idea when we do not have IPv6-RADIUS server. The process of gateway is shown in Figure 5.

First, administrator can setup a list of clients to avoid processing packets from invalid access points. When gateway starts, it uses port 1812 for receiving authentication request and port 1813 for receiving accounting request. If gateway receives an IPv6 RADIUS packet from an invalid host, it will drop this packet. Otherwise, gateway parses this packet and logs it. By this way, administrator can analyze packets which are exchanged between access points and RADIUS server. In next step, gateway encapsulates RADIUS messages into UDP and places them into the payload of IPv4 packet. After that, the gateway sends this packet to the IPv4-RADIUS server. When the gateway receives the RADIUS packet from IPv4-RADIUS server, it encapsulates RADIUS messages into UDP and places them into

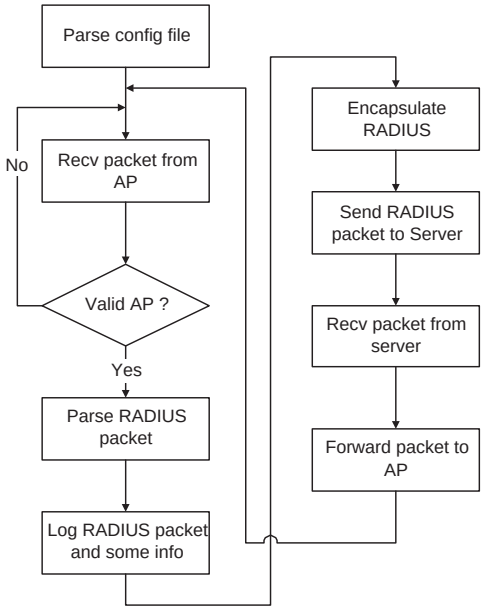


Figure 5. The process of IPv4/IPv6 RADIUS gateway

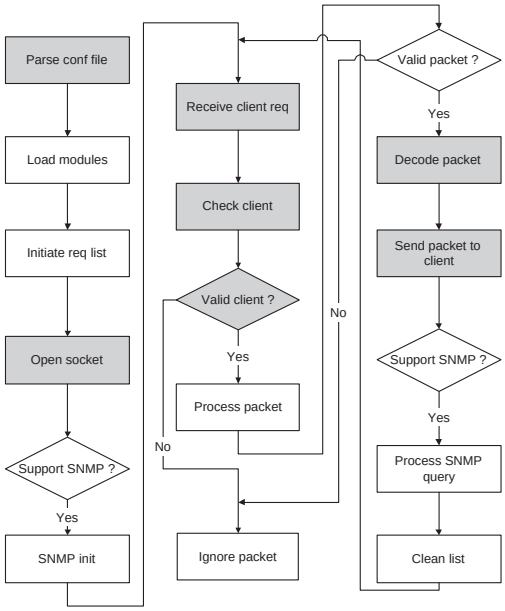


Figure 6. The process of FreeRADIUS

the payload of IPv6 packet. Now, the gateway can send this packet to access point. Up to present, the communication between the access point and the IPv4-RADIUS server is completed one time, and then the gateway goes back "Recv packet from AP" step to wait another request coming.

2.4 RADIUS Server

FreeRADIUS is one of the most popular free RADIUS servers available today. It is an Internet authentication daemon, which implements the RADIUS protocol, as defined in RFC 2865 and others. It provides port 1812 for authentication, port 1813 for accounting, port 1814 for proxy, and services for SNMP. In authentication mechanisms, FreeRADIUS supports PAP, CHAP, EAP-TLS, EAP-MD5, etc. Using it allows authentication and authorization for a network to be centralized, and minimizes reconfiguration which has to be done when adding or deleting new users. FreeRADIUS is available for a wide range of platforms, including Linux, FreeBSD, OpenBSD, OSF/Unix, and Solaris. In this paper, we will focus on FreeRADIUS running under Linux.

The operation of FreeRADIUS is shown in Figure 6.

From the point of view of protocol layer, it is easy to replace IPv4 with IPv6. But this idea triggers a series of problems. Because IPv4 and IPv6 have many different features, and the source code of FreeRADIUS has a lot of places which are related to IP address or network prefix, we can not simply replace IPv4 with IPv6. Besides, there are many functions using IP structure as parameters, if we modify the type of these parameters, we have to find out other functions that related to these functions. Gray block diagrams in Figure 6 are parts we have modified, and the following steps illustrate problems of these parts in more detail:

1. IP address:

   First, IPv4 structure and IPv6 structure are different. Second, because IPv4 addresses are 32 bits but IPv6 addresses are 128 bits, functions such as *htonl* and *ntohl* are not suitable for the IPv6 address. Besides, the representation of IPv4 addresses and the representation of IPv6 addresses are different, so we cannot use the same methods to deal with IP addresses.

2. Network prefix:

   Netmask is used to mask IP address in order to compute the subnet of the IP address. In general, it uses 32-bit unsigned integer to store IPv4 network netmask. Because the size of IPv6 address is 128-bit, we have to use 128-bit prefix to mask it if we want to compute the subnet of this IPv6 address. This will trigger some problems.

In the following we illustrate how we modify the FreeRADIUS. The modifications can be divided into three parts, including structures, variables, and functions.

1. Structures

FreeRADIUS defines its RADIUS client structure or other to record information which system would use. Relation between some structures quite closes. Therefore, we have to reduce the modification of structure as possible as we can, or we will face a real challenge. We use an example to illustrate.

```
typedef struct radclient {
        struct in6_addr         ipaddr;
        uint32_t                netmask[4];
        char                    longname[256];
        u_char                  secret[32];
        char                    shortname[32];
        char                    nastype[32];
        char                    login[32];
        char                    password[32];
        struct radclient        *next;
} RADCLIENT;
```

Figure 7. RADIUS client structure

As Figure 7, it is a structure to record information of valid clients. In `ipaddr`, we had replaced in_addr with in6_addr. In `netmask`, we used four 32-bit unsigned integers to replace one 32-bit unsigned integer.

2. Functions

We can divide functions related IP address into two categories. In first category, functions use IP address as parameter and deal with IP address problems, such as `ip_ntoa`. In second category, functions do not use IP address or network prefix as parameter but deal with IP address problems, such as functions responsible to read configuration files included IP address and network prefix. In this section, we use functions in second category as our example. System reads ”clients” and ”clients.conf” files to general the client list. It validates the sender by checking sender’s IP address. If sender doesn’t match any address in the client list, system sends an Access-Reject packet to sender. Therefore, if sender is IPv6 host, the client list should be modified. Here we show an example to explain why it should be modified.

The clients file includes IP address and network prefix. System has to store them into the structure of client list in order to compute the sender’s IP address is valid. As Figure 8, it responsible to the generation of 128-bit prefix. The following steps show the operation of Figure 8.

(a) First, we use four 32-bit unsigned integers to store 128-bit prefix and set value 1 in all bits.

(b) If prefix value in configuration file is more than 128 or less than 0, program returns error message. If prefix value is 128, program needn’t to deal with it.

(c) Due to each unsigned integer is 32-bit, we needn’t to shift bit if prefix value is between 0 and 127 and divisible by 32.

(d) If prefix value is not divisible by 32, it exist one 32-bit unsigned integer that should be modified. We use remainder as the number of times and use the method of ”shift bit” to get the correct value.

```
for(j=0;j<4;j++) mask[j] = ~0;

        if (p) {
                int i, mask_length;

                *p = '\0';
                p++;

                mask_length = atoi(p);
                if ((mask_length <= 0) || (mask_length > 128)) {
                    radlog(L_ERR, "%s[%d]: Invalid value '%s' for IP network mask.",file, lineno, p);
                            return -1;
                    }
                if (mask_length < 128 ){
                        if (mask_length%32 == 0) mask[mask_length/32] = 0;
                        else                     mask[mask_length/32] = (1 << 31);
                        for (i = 1; i < mask_length%32 ; i++) {
                                mask[mask_length/32] |= (mask[mask_length/32] >> 1);
                        }
                        for (j = 1 + mask_length/32 ; j < 4 ; j++) mask[j] = 0;
                }
        }
```

Figure 8. The process of reading "clients" file

3 Experiment Environment

3.1 Development Environment

The experiment environment is shown in Figure 9. The following items illustrate system components in more detail.

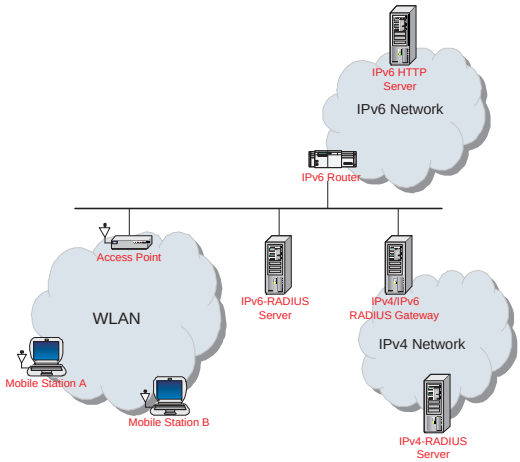


Figure 9. Experiment environment

1. Mobile station:

In mobile station A, we used Mandrake Linux 9.0 as the platform and used xsupplicant [12] software to support IEEE 802.1x functionality. Because xsupplicant software only supports CISCO adapters, we use CISCO AIRONET 340 as our wireless LAN adapter. In mobile station B, we used Microsoft Windows 2000 as the platform. In addition, we used INTEREPOCH wireless LAN adapter and its IEEE 802.1x utility. Finally, we used Microsoft msripv6-bin-1.4 to let Microsoft Windows 2000 support IPv6 protocol.

2. Access point:

   We used RedHat Linux 7.3 as the platform and HostAP software. The version of HostAP we modified is hostap-2002-10-12. We use Z-COM XI-325 as our wireless LAN adapter.

3. RADIUS server:

   There are two RADIUS servers, one is IPv4-RADIUS server, and the other is IPv6-RADIUS server. They used RedHat Linux 7.3 as the platform. The version of FreeRADIUS is freeradius-snapshot-20021028. In order to support the EAP-TLS protocol, we used openssl-SNAP-20021027 version.

3.2 Implementation Results

In general, IEEE 802.1x utility provides two authentication mechanisms, EAP-MD5 and EAP-TLS. Thus, we used these two authentication mechanisms and different operation systems to test our system. Six cases are tested in our experiments as follows.

1. EAP-MD5:

   Case 1: Client (Windows 2000) + AP + Gateway + IPv4-RADIUS Server

   Case 2: Client (Windows 2000) + AP + IPv6-RADIUS Server

2. EAP-TLS:

   Case 3: Client (Linux) + AP + Gateway + IPv4-RADIUS Server

   Case 4: Client (Linux) + AP + IPv6-RADIUS Server

   Case 5: Client (Windows 2000) + AP + Gateway + IPv4-RADIUS Server

   Case 6: Client (Windows 2000) + AP + IPv6-RADIUS Server

We use ping and HTTP to verify if mobile stations can access Internet resources after authentication. The following figures show the results of each host.

1. Mobile Station:

   First, we send HTTP requests from mobile station A. Because mobile station A is an unauthorized client, packet can not pass through our access point. The result is shown in Figure 10. Then, Figure 11 shows the whole porcess of using EAP-TLS mechanism to authenticate. After authentication, we send HTTP requests to verify if we can access Internet. As Figure 12, we see that mobile station A can access Internet resources after authentication.

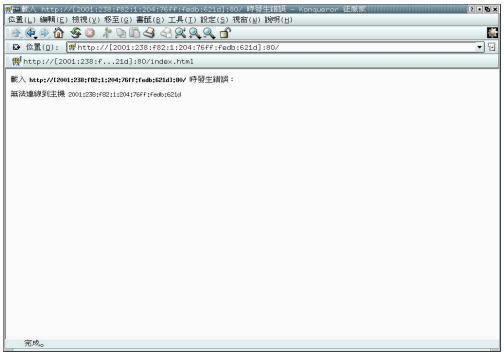


Figure 10. Browsing an IPv6 web site before authentication

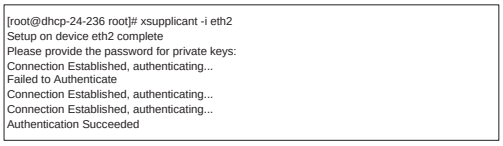


Figure 11. EAP-TLS authentication information

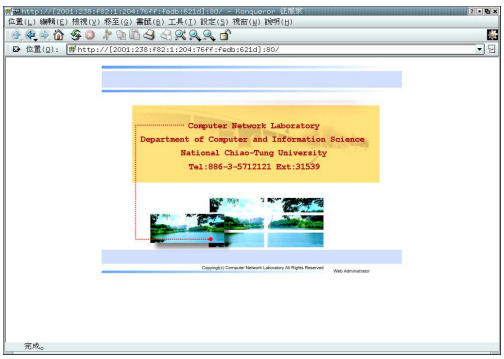


Figure 12. Browsing an IPv6 web site after authentication

2. Access Point:

Figure 13 shows how access point deals with authentication frames. From this figure, we see that the access point can communicate with IPv6-RADIUS server properly. Besides, it can send RADIUS packet with NAS-IPv6-Address attribute by using the parameter ”-O”.

```
[root@netlab39 hostapd]# ./hostapd -x -o 140.113.167.235 -O
2001:238:f82:2:200:e2ff:fe7f:56e0 -A 2001:238:f82:2:204:76ff:fedb:64ed -s whatever wlan1

Using interface wlan1ap with hwaddr 00:60:b3:f1:fa:94 and ssid 'test'
Flushing old station entries
Station 00:06:f4:00:94:2e authenticated (open system)
Station 00:06:f4:00:94:2e associated (aid 1)
IEEE 802.1X: Start authentication for new station 00:06:f4:00:94:2e
IEEE 802.1X: Unauthorizing station 00:06:f4:00:94:2e

Sending data to RADIUS server...
Received 84 bytes from RADIUS server: 2001:238:f82:2:204:76ff:fedb:64ed

Sending data to RADIUS server...
Received 1120 bytes from RADIUS server: 2001:238:f82:2:204:76ff:fedb:64ed

Sending data to RADIUS server...
Received 872 bytes from RADIUS server: 2001:238:f82:2:204:76ff:fedb:64ed

Sending data to RADIUS server...
Received 131 bytes from RADIUS server: 2001:238:f82:2:204:76ff:fedb:64ed

Sending data to RADIUS server...
Received 160 bytes from RADIUS server: 2001:238:f82:2:204:76ff:fedb:64ed

IEEE 802.1X: Authorizing station 00:06:f4:00:94:2e
IEEE 802.1X: Unauthorizing station 00:06:f4:00:94:2e
IEEE 802.1X: Unauthorizing station 00:06:f4:00:94:2e
IEEE 802.1X: Unauthorizing station 00:06:f4:00:94:2e
Signal 2 received - terminating
Flushing old station entries
Deauthenticate all stations
[root@netlab39 hostapd]#
```

Figure 13. Messages of access point

3. IPv4/IPv6 RADIUS Gateway:

   Both the list of valid clients and messages of receiving/sending RADIUS packets are presented in Figure 14.

```
[root@route1 root]# ./Gateway -R 140.113.167.196
The adress list of valid IPv6 clients:
2001:238:f82:2::1
2001:238:f82:2:204::1
2001:238:f82:0:1::1
2001:238:f82:2:200:e2ff:fe7f:56e0

Receiving an IPv6 packet!!
Check client IP address!!
A valid client: 2001:238:f82:2:200:e2ff:fe7f:56e0 , accept packet!!
Packet type: Access-Request RADIUS packet

Sending packet to RADIUS server: 140.113.167.196

Receiving Access-Challenge RADIUS packet from RADIUS server 140.113.167.196

Sending packet to client 2001:238:f82:2:200:e2ff:fe7f:56e0

Receiving an IPv6 packet!!
Check client IP address!!
A valid client: 2001:238:f82:2:200:e2ff:fe7f:56e0 , accept packet!!
Packet type: Access-Request RADIUS packet

Sending packet to RADIUS server: 140.113.167.196

Receiving Access-Challenge RADIUS packet from RADIUS server 140.113.167.196

Sending packet to client 2001:238:f82:2:200:e2ff:fe7f:56e0
```

Figure 14. Messages of IPv4/IPv6 RADIUS gateway

4. IPv6-RADIUS Server:

   Figure 15 shows the process of dealing with RADIUS packets in the IPv6-RADIUS server. From this figure, we see that the IPv6-RADIUS server can receive RADIUS packets from IPv6 host and send back properly.

```
...
Listening on IP address *, ports 1812/udp and 1813/udp, with proxy on 1814/udp.
Ready to process requests.
rad_recv: Access-Request packet from host 2001:238:f82:2:200:e2ff:fe7f:56e0:32768, id=0, length=170
listaddr:fe3f mask:ffffffff recvaddr:38020120
listaddr:38020120 mask:ffffffff recvaddr:38020120
listaddr:200820f mask:ffffffff recvaddr:200820f
listaddr:0 mask:0 recvaddr:ffe20002
listaddr:0 mask:0 recvaddr:e0567ffe
        User-Name = "win2000"
        NAS-IP-Address = 140.113.167.235
        NAS-IPv6-Address = 0x200102380f8200020200e2fffe7f56e0
        NAS-Port = 1
        Called-Station-Id = "00-60-B3-F1-FA-94:test"
        Calling-Station-Id = "00-06-F4-00-94-2E"
        Framed-MTU = 2304
        NAS-Port-Type = Wireless-802.11
        Connect-Info = "CONNECT 11Mbps 802.11b"
        EAP-Message = "\002\003\000\014\001win2000"
        Message-Authenticator = 0xff1c6f4613af3423d25e2a6c7b9d30e4
modcall: entering group authorize
  modcall[authorize]: module "preprocess" returns ok
rlm_chap: Could not find proper Chap-Password attribute in request
  modcall[authorize]: module "chap" returns noop
  modcall[authorize]: module "eap" returns updated
    rlm_realm: No '@' in User-Name = "win2000", looking up realm NULL
    rlm_realm: No such realm NULL
  modcall[authorize]: module "suffix" returns noop
    users: Matched win2000 at 90
  modcall[authorize]: module "files" returns ok
modcall: group authorize returns updated
  rad_check_password:  Found Auth-Type EAP
auth: type "EAP"
modcall: entering group authenticate
rlm_eap: processing type md5
rlm_eap_md5: Issuing Challenge
  modcall[authenticate]: module "eap" returns ok
modcall: group authenticate returns ok
Sending Access-Challenge of id 0 to 2001:238:f82:2:200:e2ff:fe7f:56e0:32768
        EAP-Message = "\001\004\000\026\004\020a$\212\224Y\203\004Gl\273\016rZX\201\304"
        Message-Authenticator = 0x00000000000000000000000000000000
        State =
0x678d14922eef40402bba115d7eedb47db47bd33e48821cc3b5b015cc96d13ebcdc21bec8
Finished request 0
Going to the next request
--- Walking the entire request list ---
Waking up in 6 seconds...
rad_recv: Access-Request packet from host 2001:238:f82:2:200:e2ff:fe7f:56e0:32768, id=1, length=225
...
```

Figure 15. Messages of IPv6-RADIUS server

4 Conclusions

IPv6 protocol has some advantages over IPv4 protocol, and most OS have already supported IPv6 protocol, such as Linux, Windows XP, and FreeBSD. In addition, it has more and more IPv6 networks that coexist with IPv4 networks. In this paper, we have implemented an IPv6 authentication system based on IEEE 802.1x and RADIUS protocol. We modified HostAP software, which is used to simulate access point, to support IPv6 RADIUS protocol and can communicate with IPv6-RADIUS server. Besides, we have implemented an IPv4/IPv6 RADIUS gateway that is responsible to the communication between access point and IPv4-RADIUS server. Finally, we modified FreeRADIUS software to become an IPv6-RADIUS server that can run over IPv6 networks properly. Thus, we can provide authentication services to users in IEEE 802.11 wireless networks by using this IPv6 authentication system.

In the future, we are planning to add functions into HostAP software to support accounting capability when using IEEE 802.1x authentication. Besides, we want to modify FreeRADIUS as a dual mode RADIUS server. This means that RADIUS server can run over IPv4 networks and IPv6 networks simultaneously. Thus, this RADIUS server can supply authentication, authorization, and accounting services to IPv6 networks users as well as IPv4 networks users. Furthermore, we hope to evaluate and compare the performance of IPv4-RADIUS server and IPv6-RADIUS server in the future.

References

[1] ”Part 11:Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications”, *ANSI/IEEE Std 802.11*, 1999 Edition, http://standards.ieee.org/getieee802/802.11.html

[2] ”Port-
Based Network Access Control”, *IEEE std 802.1x*, 2001, http://standards.ieee.org/getieee802/802.1.html

[3] L. Blunk, and J. Vollbrecht, ”PPP Extensible Authentication Protocol (EAP)”, *RFC-2284*, March 1998

[4] B. Aboba, and D. Simon, ”PPP EAP TLS Authentication Protocol”, *RFC-2716*, October 1999

[5] C. Rigney, S. Willens, A. Rubens, and W. Simpson, ”Remote Authentication Dial In User Service (RADIUS)”, *RFC-2865*, June 2000

[6] C. Rigney, W. Willats, P. Calhoun, ”RADIUS Extensions”, *RFC-2869*, June 2000

[7] FreeRADIUS. [Online]. Available: http://www.freeradius.org/

[8] S. Deering, and R. Hinden, ”Internet Protocol, Version 6 (IPv6) Specification”, *RFC-1883*, December 1995

[9] B. Aboba, G. Zorn, and D. Mitton, ”RADIUS and IPv6”, *RFC-3162*, August 2001

[10] HostAP. [Online]. Available: http://hostap.epitest.fi/

[11] Mattbew S. Gast, ”802.11 Wireless Networks: The Definitive Guide”, *O’REILLY*, April 2002

[12] xsupplicant. [Online]. Available: http://www.open1x.org/

附件二

Energy-Aware, Load Balanced Routing Schemes for Sensor Networks*

Shih-Chang Huang and Rong-Hong Jan†
National Chiao Tung University
Department of Computer and Information Science
Hsinchu, 30050, Taiwan

Abstract

This paper presents two energy-aware, load balanced routing schemes, called as maximum capacity path (MCP) scheme and MCP with path switching (MCP-PS) scheme, for sensor networks. In the MCP scheme, the sensor network is constructed into a layered network at first. Based on the layered network, every sensor node selects a shortest path with maximum capacity to sink. In MCP-PS, the node may switch its routing path to its sibling neighbors in order to share the traffic. The simulation results show that our MCP and MCP-PS schemes can achieve a better load-sharing and better endurance on network lifetime.

Keywords: *Wireless sensor networks, Energy aware routing, Multi-path routing, Maximum capacity path.*

1 Introduction

The fast progress of micro-electro-mechanical systems (MEMS) technology and wireless communications has enabled us to deploy a large number of low-cost, low-power and networked sensors in a dangerous area or path-less region such as battlefield, disaster area, and exploring space to act as pre-warning sentinels, environment monitors or location information collectors. The power of these tiny sensor nodes comes from their equipped batteries. Thus, how to use the limited battery energy efficiently is a crucial research issue in sensor networks.

Many power-saving researches have been proposed to save the precious energy of sensor nodes. They save energy in different aspects such as reducing the power spending on modulation circuits [1], managing the power usage on MAC layer of sensor nodes [2, 3]. These power-saving mechanisms focus on an individual device. However, the power-saving of individual sensor node is not enough in sensor networks, the power-saving of collaborative works of sensor nodes shall also be considered. Because sensor nodes have limited transmitting range, only a small subset of them can communicate with sink node directly in which sink node is a central controller to handle the operation of sensor nodes. In most of the cases, the collecting data of a sensor node must be forwarded by others to reach the sink. And these relaying operations consume a great deal of energy. Once the heavy relay operations run out of some sensor nodes' energy, the network may be separated and the sensing data cannot be returned. Therefore, developing energy efficiency and load balance routing algorithms to prolong the network operating time gradually becomes a key topic in sensor networks.

Routing algorithms that use fixed paths in traditional wired network [4, 5] are not suitable for sensor networks which have limited resources. Sensor nodes that locate in the fixed path suffer severe energy consumption and exhaust quickly because they provide relaying services to a huge number of compatriots. This extreme unfair load-sharing between the sensor nodes on the path and the other nodes incurs the network separating. In addition, applying the fixed paths routing mechanism to sensor networks [6, 7] must pay the costs of periodically re-establishing the paths because sensor networks do not have pre-planning infrastructure usually.

For wireless sensor networks' routing, a simple routing method is flooding. However, flooding mechanism consumes too much energy on relaying unnecessary traffic. To solve this problem, source routing alike schemes [8, 9] are proposed for sensor networks. But they cannot work well if the number of hops from sensor node to sink is large. The overhead for delivering source routing information cannot be negligible. Cluster-based schemes [10, 11] which form sensor nodes to clusters or a chain are also introduced to gather data. In cluster-base schemes, every sensor node must be able to adapting it radio power, which increases the

*This work was supported in part by the Lee and MTI Center for Networking Research, NCTU, Taiwan and the Ministry of Education and National Science Council, Taiwan, ROC, under grants 89-E-FA04-1-4 and NSC 92-2219-E-009-012, respectively.

†Corresponding Author. Fax: 886-3-5721490; e-mail: rhjan@cis.nctu.edu.tw

manufacture costs of each sensor node. Becides, the data delivering delay is long and not garanteeded. Considering the load balance of sensor nodes and the limited memory spaces, dynamic multi-path routing schemes [12, 13] seem suitable for sensor networks.

In multi-path routing schemes [12, 13], sensor nodes have multiple paths to forward their data. Each time data sends back to sink, sensor node picks up one of its feasible paths based on special constrains such as maximum available energy, minimum delay times, or security. Multi-path routing has the advantage on sharing energy depletion between all sensor nodes. However, the drawback of the multi-path routing proposed by [12, 13] is that sensor nodes only keep a local view on energy usage and the nodes in network cannot have an even traffic dispatch. Thus, this paper focuses on how to get a global view on energy of sensor nodes by exchanging the local information of each sensor node and gives a better load sharing over all sensor nodes.

An energy-aware multi-path routing scheme, called as maximum capacity path scheme (MCP scheme), is proposed in this paper. In the MCP scheme, the sensor network is constructed as a layered network at first. Based on the layered network, every sensor node selects a shortest path with maximum capacity to sink. In order to improve the performance of MCP scheme, a path switching function is added to MCP scheme, denoted as MCP with path switching (MCP-PS) scheme. In MCP-PS, a node can switch the routing path to its neighbors in order to sharing the traffic. Both MCP and MCP-PS schemes exhibit a better load sharing and better endurance on network lifetime than the schemes proposed by [13].

The rest of this paper is organized as follows. In section 2, we will show layered network model for multi-path routing. Section 3 describes the MCP scheme. Section 4 shows MCP-PS scheme. The simulation results are given in section 5 and conclusion in section 6.

2. Layered network model

In general, a wireless sensor network can be transformed into a *graph* $G = (V, E, s)$ in which each node in set $V \setminus \{s\}$ stands for a sensor node, an edge (u, v) is in E if sensor nodes u and v can communicate each other directly, and node $s \in V$ represents the sink. Multi-path routing scheme constructs sensor network G into a shortest path network, called *layered networks*, and sends the sensing data in this network. Formally, the layered network N is defined as follows. We determine the exact hop distance h from a sensor node to sink in G. The layered network consists of those edges (u, v) in G satisfying the condition $h_u = h_v + 1$. For example, consider a wireless sensor network G shown in Fig. 1(a). The number beside each node represents its exact hop distance. Fig. 1(b) shows the layered network N of G. Observe that by definition every path from any node to the sink in the layered network N is a shortest path in G.

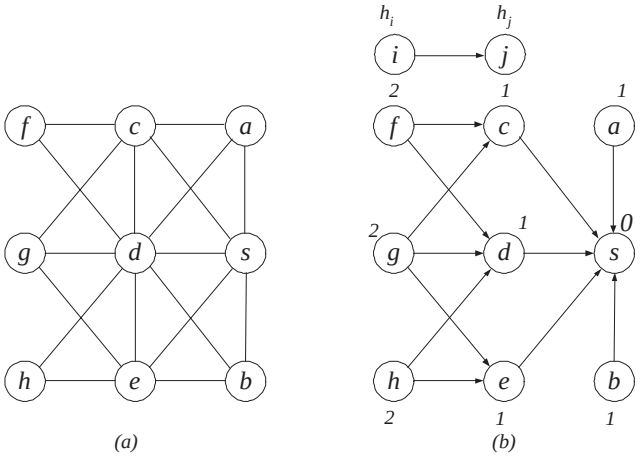


Figure 1. Forming layered networks: (a) sensor network G; (b) corresponding layered network N.

The layered network can be constructed as follows. Let variable h_v be the hop count to the sink maintained by node v. Initially, the sink sets its $h_s = 0$ and the every other node u sets its h_u to infinity. The sink periodically broadcasts poll message with its hop count values h_s to its neighbors. Note that poll-reply communication model is adopted in this paper. When a node u receives a poll message from node v, it extracts the hop count value h from the poll message. The following comparisons are conducted:

1. If $h > h_u - 1$, node u does nothing.
2. If $h = h_u - 1$, node u builds an in-bound link to the node v.
3. If $h < h_u - 1$, node u deletes the existing in-bound links and builds an in-bound link to node v. Then, node u sets $h_u = h + 1$, and re-broadcasts the poll message with hop count value h_u to its neighbors.

By broadcasting poll messages and comparing h with h_u step by step, the layered network can be constructed.

Figure 2 gives an illustrated example for building a layered network. In Figure 2(a), all sensor nodes initiate their levels to infinity. In Figure 2(b), sink s broadcasts a poll message with $h = 0$. Sensor nodes a and b are within the transmission range of the sink and they will receive poll message originated from the sink. Since $0 < \infty$, nodes a and b build in-bound links to sink s, set $h_a = h + 1 = 1$ ($h_b = 1$), and forward the poll message with hop count numbers $h_a = 1$ ($h_b = 1$) to their neighbors. In Figure 2

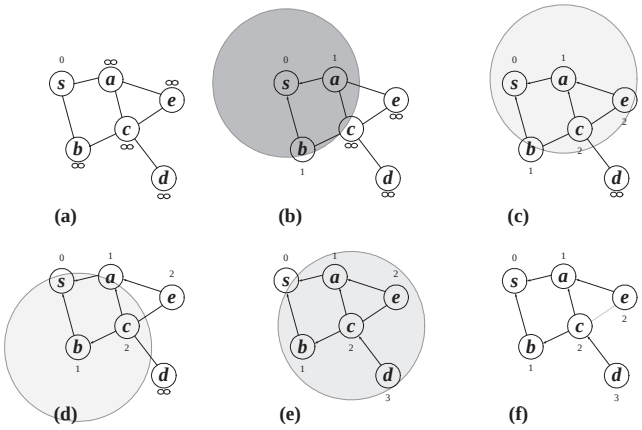


Figure 2. Layered network

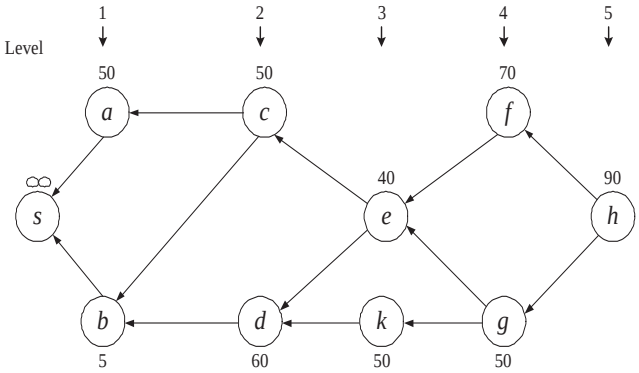


Figure 3. Example of path selection in the layered network

(c), nodes c and e receive poll message from node a. Since $1 < \infty$, nodes c and e set $h_c = h_e = 2$ and build in-bound links to node a, respectively. In Figure 2 (d), nodes a and c receive poll message from node b. Node a discards this poll message since $h > h_a - 1$. Node c builds in-bound link to node b since $h = h_c - 1$. Finally, the layered network is constructed and showed in Figure 2(f).

3 Maximum capacity path scheme

Note that a sensor node in the layered network may have multiple shortest path to reply the sensing data to sink. For example, consider a layered network N of G as shown in Fig. 3. The number beside each node represents its available energy. When sensor node e at level 3 has a data packet to send, it has three routing paths: $e \rightarrow c \rightarrow a \rightarrow s$, $e \rightarrow c \rightarrow b \rightarrow s$, and $e \rightarrow d \rightarrow b \rightarrow s$. Suppose that node e selects a neighbor node with maximum available energy as its forwarder, say node d. That is, node e selects path $e \rightarrow d \rightarrow b \rightarrow s$ to forward the data. However, the available energy of node b is very low and then node b will run out of its energy rapidly.

In order to avoid this fault, we proposed a path selection scheme, called as maximum capacity path scheme, for each sensor node to select a routing path with maximum capacity to sink. Let $c(v) \geq 0$ denote the available energy of node v in N and assume that $c(s) = \infty$. Define the capacity of a routing path $P = v_0, v_1, \ldots, v_k, s$ as minimum node energy in P. The maximum capacity path scheme is to determine a maximum capacity path from a specified sensor node to sink in the layered network. For example, as shown in Fig. 3, the capacities of paths $e \rightarrow c \rightarrow a \rightarrow s$, $e \rightarrow c \rightarrow b \rightarrow s$, and $e \rightarrow d \rightarrow b \rightarrow s$ are 50, 5, and 5, respectively. Thus, the maximum capacity path scheme will select path $e \rightarrow c \rightarrow a \rightarrow s$ as forwarding path for node e. That is, node e sends data packets along path $e \rightarrow c \rightarrow a \rightarrow s$. In general, suppose that sensor node v has k in-bound links $(v, u_1), (v, u_2), \ldots, (v, u_k)$. Let $p(w)$ denote the maximum capacity value of maximum capacity path P from node w to sink s. Thus, sensor node v selects node u^* as forwarder to forward its data such that $p(u^*) = \max\{p(u_1), \ldots, p(u_k)\}$. Then, node v updates its $p(v)$ by $p(v) = \min\{c(v), p(u^*)\}$.

3.1 Maximum capacity path creation

In order to achieve maximum capacity path scheme, each sensor node v maintains a local table to record its in-bound links $(v, u_1), (v, u_2), \ldots, (v, u_k)$ and the corresponding maximum capacity values $p(u_1), \ldots, p(u_k)$. In addition, node v sets $p(v) = \min\{c(v), p(u^*)\}$ where $p(u^*) = \max\{p(u_1), \ldots, p(u_k)\}$. The maximum capacity value is propagated along with the poll messages while layered network is building. Initially, sink s sends poll message with $p(s) = \infty$. When node v creates an in-bound link (v, u) to u, node v checks to see whether $p(u)$ is greater than $p(u^*)$ or not where node u^* is the current forwarder of node v. If $p(u) > p(u^*)$, then node v changes its forwarder to node u, sets $p(u)$ to $p(u^*)$ and updates $p(v) = \min\{c(v), p(u)\}$. Otherwise, node v does nothing.

Figure 4 shows an example for maximum capacity path scheme. Figure 4(a) shows a sensor network G. The available energy $c(v)$ is beside each node v. In Figure 4(b), sink s broadcasts a poll message with $h = 0$ and $c(s) = \infty$. Sensor nodes a and b receive the poll message from the sink and create in-bounds (a, s) and (b, s), respectively. Node a (Node b) sets $p(s) = \infty$ and $p(a) = \min\{p(s), c(a)\} = 30$ ($p(b) = \min\{p(s), c(b)\} = 40$). In Figure 4(c), nodes c and e receive poll message with $h = 1$ and $c(a) = 30$ from node a. Since $1 < \infty$, nodes c and e set $h_c = h_e = 2$ and build in-bound links (c, a) and (e, a), respectively. Node c (Node e) sets $p(a) = 30$ and $p(c) = \min\{p(a), c(c)\} =$

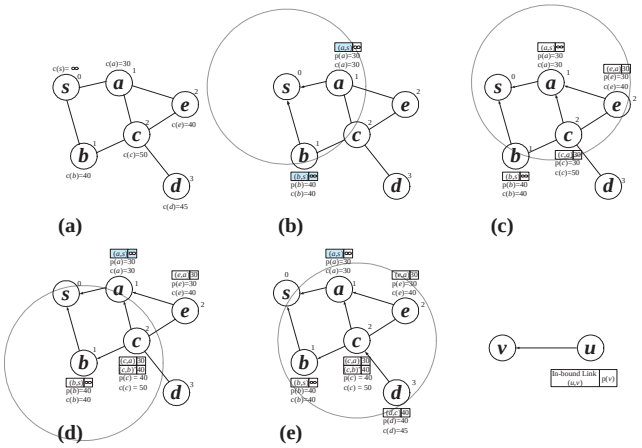


Figure 4. Example of maximum capacity path creation in layered network

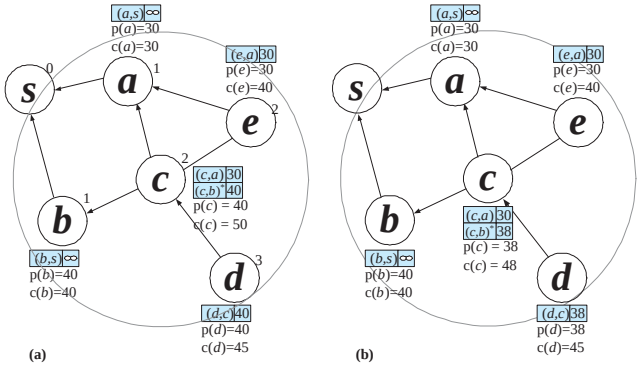


Figure 5. Maintenance of maximum capacity path

30 ($p(e) = \min\{p(a), c(e)\} = 30$). In Figure 4(d), nodes a and c receive poll message from node b. Node a discards this poll message since $h > h_a - 1$. Node c builds in-bound link (c, b) since $h = h_c - 1$. Node c sets $p(b) = 40$. Since $p(b) > p(a)$, node c selects node b as forwarder and sets $p(c) = \min\{p(b), c(c)\} = 40$. Finally, node d creates an in-bound link (d, c) and sets $p(d) = 40$ as shown in Figure 4(f).

3.2 Maximum capacity path maintenance

Note that data transmission and receipt consume the energy of sensor nodes. In this paper, the energy consumption of each delivery is assumed to be a constant δ and known in advance. Every sensor node v shall update its energy $c(v)$ and recalculate maximum path capacity $p(v)$ after data is transmitted. We can take advantage of the overhearing of wireless communication. That is, every sensor node v adds its updated maximum path capacity $p(v) - \delta$ in the data packet when it sends the data. Then, node u can learn the maximum path capacity $p(v)$ from the message if node u has an in-bound link to to v.

Formally, the maintenance of maximum capacity path is given as follows. If node y at level ℓ relays a message with $p(y) - \delta$ to node x at level $\ell - 1$, then every node v at level $\ell + 1$ with an in-bound to node y can hear the message and learn $p(y) - \delta$ from this message. Next, node v updates $p(y) = p(y) - \delta$ in the entry of in-bound link (v, y) in the local table. Then, node v checks to see if forwarder changes or not. With this learning mechanism, each sensor node in the network can maintain the maximum capacity path.

For example, as shown in Figure 5(a), node c sends a message to b with $p(c) = 40 - 2 = 38$. Then, node d learns $p(c) = 38$ from the message and updates its local table (see Figure 5(b)). Note that node c also updates its $p(c) = 38$ and $c(c) = 48$.

4 MCP scheme with path switching

In order to improve the load-sharing of MCP scheme, we add path switching function to MCP scheme, call as MCP scheme with path switching (MCP-PS). In MCP-PS scheme, every sensor node keeps an extra table to record the maximum capacity values of its sibling neighbors. A node w is said to be a sibling neighbor of v if nodes w and v are in the same level and $(v, w) \in G$. The maximum capacity values can also be learned by examining the data packets from the sibling neighbors as in MCP scheme. In MCP-PS scheme, sensor node v checks to see if there exists a sibling neighbor w such that $p(u) < p(w)$ or not, where node u is a forwarder of v. If answer is yes, node v changes its forwarder to sibling neighbor w; otherwise, selects u as forwarder as in MCP scheme.

Note that MCP-PS scheme consumes more energy than MCP scheme because MCP-PS spends extra energy to forward data packet to its sibling neighbor and its routing path may not be a shortest path. Howerevr, MCP-PS scheme chooses a higher capacity path to forward data packet. Thus, it can give a better load-sharing solution and prolong the network lifetime.

5 Simulation results

5.1 Performance metrics and environment Setup

In our simulation environment, time for first node to die is used to evaluate the performance of our routing schemes and compare with algorithms proposed in [11]. The lifetime is defined as the first node runs out of energy. In the

Table 1. The average extra hop needed by the MCP-PS scheme.

	area size		
	3×3 km^2	4.5×4.5 km^2	6×6 km^2
100 nodes	0.896	1.915	1.236
200 nodes	0.868	2.947	3.497

simulation, all nodes return their data to the sink periodically. Instead of using the clock time, we use number of turns to present the lifetime of network. A *turn* is defined as all nodes in the network finish to return their data to sink once. The time interval between two turns is supposed large enough for last node to return its data.

Three different size of deploying regions are simulated. They are $3 \times 3, 4.5 \times 4.5$ and 6×6 kilometer square areas. In each the area, 100 and 200 nodes are deployed by uniform distribution. And totally, there are 1000 different deploying topologies (cases) in each of the six cases. Nodes are assumed to be stationary after being deployed. And at each turn, they return their data in random sequence. A new turn can not be started before all nodes have finished reporting their data in the previous turn. The initial energy of each node is uniform distributed in $[2000, 3000]$. We also assume that the length of returning packet is fixed so that the energy consumption of the transmitting and receiving operations for sensor nodes is constant (in our simulation environment, 3 units for transmitting and 0.1 for receiving). A clear channel is assumed and data loss rate is set to zero. In addition, the radio range of each sensor node is set to 750 meters and its coverage area is assumed to be a perfect circle and the symmetric communication link is used.

5.2 Numerical results

A comparison of the network lifetime (i.e., number of turns finished before the first node to die) was made for four schemes: MCP, MCP-PS, Multi-Path (MP) [12], and Multi-Path with Energy-Aware (MP-EA) [13] schemes. Figures 6-8 show the number of turns finished before the first node to die for four schemes with 100 sensor nodes deploying in the areas of $3 \times 3, 4.5 \times 4.5$ and 6×6 km^2, respectively. Figures 9-11 show the number of turns finished for 200 sensor nodes. The number of turns finished are sorted in increasing order. These figures show that MCP-PS scheme achieves more turns than MCP, MP-EA and MP schemes. From Figure 6, note that 545 of 1000 different cases are greater than 100 turns for MCP-PS secheme; 453 cases for MCP scheme; 359 cases for MP-EA scheme; only 21 cases for MP scheme. However, in Figure 8, four schemes only have little difference. The reason is that network is disconnected before sensor nodes start their operations in the large

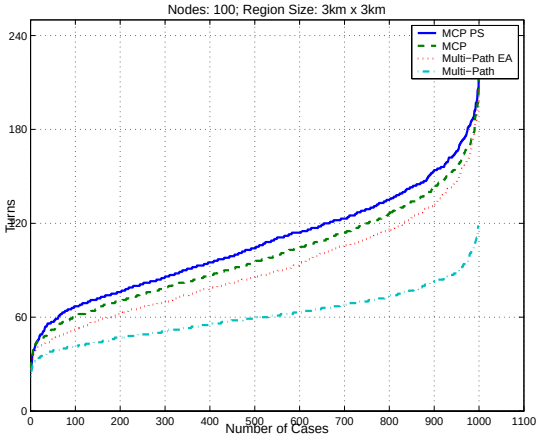


Figure 6. 100 nodes in area of 3×3 km^2

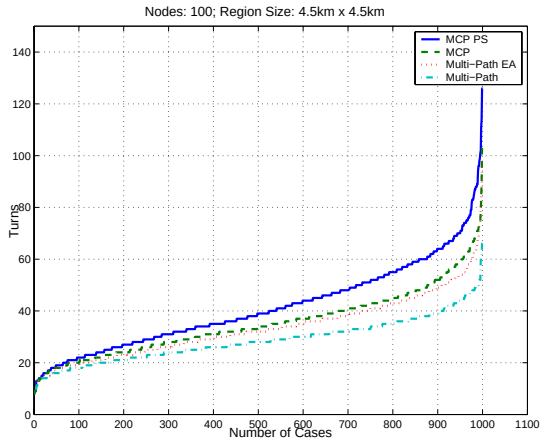


Figure 7. 100 nodes in area of 4.5×4.5 km^2

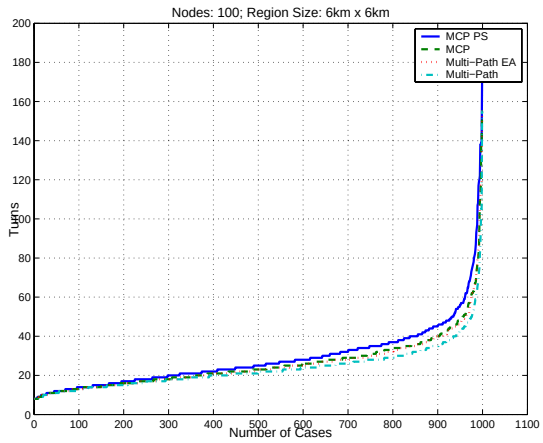


Figure 8. 100 nodes in area of 6×6 km^2

region. Only a partial set of nodes participate the network operation.

MCP's routing path is a shortest path, however, in MCP-PS scheme the shortest path is not guaranteed. Table 1 shows the average of extra hop numbers needed for each sensor node by using MCP-PS scheme. In the area of 3×3 km^2, the average extra hop needed by MCP-PS is less than one hop. In the area of 6×6 km^2, the average extra hops needed by MCP-PS are 1.236 and 3.497 for the networks with 100 nodes and 200 nodes, respectively. With little penalty of extra cost, MCP with PS can give a better network lifetime.

6 Conclusion

Sensor networks can be rapidly (ideally immediately) deployed without relying on pre-planning infrastructures. Traditional routing protocols based on fixed shortest path are not efficient in sensor networks. This paper presents two energy-aware routing schemes, MCP and MCP-PS, for sensor networks. Compared to MP and MP-EA, our MCP and MCP-PS schemes can achieve a longer network lifetime. This is because MCP and MCP-PS select the maximum capacity path for routing. Compared to MCP, MCP-PS gives a better load-sharing. However, the routing path of MCP-PS scheme may not be a shortest one. In the future, we will extend MCP-PS scheme with power saving mechanism, to prolong the network lifetime.

References

[1] C. Chien, I. Elgorriaga and C. McConaghy, "Low-power direct sequence spread-spectrum modem architecture for distributed wireless sensor networks", *Proc. of IEEE Low power electronics and design*, pp.251-254, 2001.

[2] A. Sinha, and A. Chandrakasan, "Dynamic power management in wireless sensor networks",*IEEE Design and test of computers*, pp.62-74, 2001.

[3] Y. Wei, J. Heidemann and D. Estrin, "An energy-efficient MAC protocol for wireless sensor network", *Proc. of INFOCOM 2002*, pp.1567-1576, 2002.

[4] J. Moy, "OSPF Version2," RFC 2178, Internet engineering task force, 1997.

[5] J. Moy, *OSPF: Anatomy of an internet routing protocol*, Addison-Wesley, 1998.

[6] A. Boukerche, X. Cheng and J. Linus, "Energy-aware data-centric routing in microsensor networks" *Proc. of the 8th international workshop on modeling analysis*

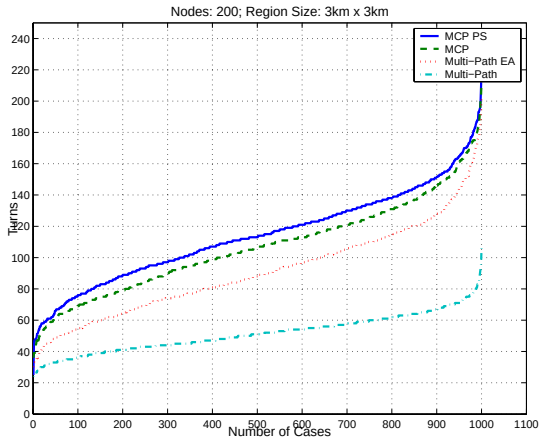


Figure 9. 200 nodes in area of 3×3 km^2

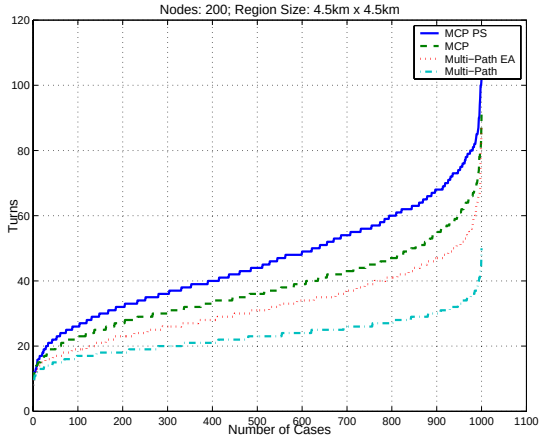


Figure 10. 200 nodes in area of 4.5×4.5 km^2

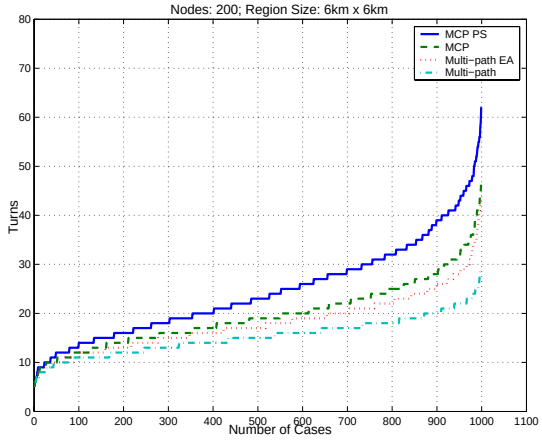


Figure 11. 200 nodes in area of 6×6 km^2

and simulation of wireless and mobile systems, pp.42-39, 2003.

[7] R.C. Shah and J.M. Rabaey, "Energy aware routing for low energy ad hoc sensor networks", *Proc. of wireless communications and networking conference*, pp.350-355, 2002.

[8] M. Younis, M. Youssef and K. Arisha, "Energy-aware routing in cluster-based sensor network", *Proc. of 10th modeling, analysis and simulation of computer and telecommunications systems*, pp.129-136, 2002.

[9] C.E. Perkins, E.M. Royer, "Ad hoc on demand distance vector routing", *Proc. of 2nd workshop on mobile computing systems and applications 1999*, pp.90-100, 1999.

[10] W.R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks", *Proc. of 33rd international conference on system sciences*, pp. 3005 - 3014, 2000.

[11] K. Du, J. Wu, D. Zhou, "Chain-based protocols for data broadcasting and gathering in the sensor networks", *Proc. of international parallel and distributed processing symposium*, pp. 22-26, 2003.

[12] X. Hong, M. Gerla, R. Bagrodia, J.k. Taek, P. Estabrook and P. Guangy, "The Mars sensor network: efficient, power aware communications", *Proc. of MILCOM*, pp. 418 - 422, 2001.

[13] X. Hong, M. Gerla, W. Hanbiao and L. Clare, "Load balanced, energy-aware communications for Mars sensor networks", *Proc. of aerospace conference*, pp. 1109-1115, vol 3, 2002.

附件三

Improving the Accuracy of Cell-Based Positioning for Wireless Networks*

Rong-Hong Jan†, Hung-Chi Chu, and Yi-Fang Lee

Department of Computer and Information Science, National Chiao Tung University, Hsinchu, 30050, Taiwan

Abstract

One fundamental issue for location-based services and applications is location-sensing problem, i.e., determining where a given node is physically located in a network. In a previous paper, we have presented a location-sensing method, called the cell-based positioning method, and its positioning accuracy for the wireless networks with a hexagonal structure and mesh structure. Unfortunately, in a real situation, a wireless network may not have a hexagonal or mesh structure. Thus, in this paper we consider the networks with an irregular structure and present an algorithm to determine the positioning accuracy of the cell-based method in irregular networks. In addition, we use the simulated annealing (SA) method to determine the locations and transmission ranges of base stations in order to achieve the best possible positioning accuracy. The simulation results show that the accuracy can be improved up to 30% by the SA method. The results are useful for deploying a wireless network for location-based applications.

Keywords: Location-sensing, location determination, location-based applications.

*This work was supported in part by the Lee and MTI Center for Networking Research, NCTU, Taiwan and the Ministry of Education and National Science Council, Taiwan, ROC, under grants 89-E-FA04-1-4 and NSC 92-2219-E-009-012, respectively.

†Corresponding Author. Fax: 886-3-5721490; e-mail: rhjan@cis. nctu.edu.tw

1 Introduction

Wireless communication is a popular trend today because it lets users communicate easily with each other at almost any time and place. One of the most important applications for wireless networks, location-based services, allows mobile users to receive services based on their geographic locations. In recent years, more and more location-based services and applications have been developed for mobile users. These services include emergency rescue, resource tracking and management, tour guide [1], location-sensitive billing, points of interest and so on.

One fundamental issue for location-based services and applications is location-sensing problem, i.e., determining the physical location of a node. Many papers [2-13] have discussed the location-sensing methods. We classify these methods into two broad categories based on where the position coordinates of a handset are determined. If the handset collects signals from the network and determines the location, it is a *handset-based* method. In contrast, if some location equipment is installed at the base-stations to collect the signal direction or timing of the handset, and then a centralized server determines the handset's location. This approach is a *network-based* method.

A. handset-based methods

Global Positioning System (GPS) [2, 3] is a typical handset-based method. It calculates the locations at the handset by measuring the time and distance between a receiver and at least three satellites. GPS has a higher position accuracy. However, times to first fix are generally longer, as GPS need to measure distances to a minimum of three satellites and the processing time is much longer. Two modified GPS methods, assisted GPS [4] and differential GPS [5, 6, 7] are presented to improve the processing speed for location determining and reduce the power consumption of mobile station.

B. Network-based methods

Angle of Arrival (AOA) and Time Difference of Arrival (TDOA) are two of the most widely known network-based location-sensing methods [8, 9]. AOA systems estimate AOA of handset signal at two or more base stations and apply simple triangulation to determine the handset's location. TDOA systems use radio frequency (RF) receivers installed at multiple base stations to measure signal time of arrival data and estimate the handset's location. Variations of these approaches are discussed in [10].

Note that network-based methods need to install location equipments at the base-stations. In contract, GPS solutions need to add the GPS receiver to handsets. Although GPS capabilities will be included in the handset chips with a little or none extra cost, end users still have to upgrade their handsets. In [13], Chu and Jan present a simple, low-cost method for location-sensing, called the cell-based location-sensing method. In the cell-based method, the handset gathers all of the base station (BS) signals that it received and transmits the BS identification (ID) to the location server. Based on these BS IDs, the server can then determine the location of the handset. Thus, the cell-based method only requires several lines of code on the Subscriber Identity Module (SIM) card to get the list of BSs within range. This code can be embedded on the SIM when the SIM is issued or delivered over-the-air to the SIM via Short Messaging Service (SMS) messaging. That is, the cell-based method requires no changes to either the existing wireless network architecture or the handset devices, and it can be applied to Global System for Mobile Communications (GSM) right now.

However, only wireless networks with hexagonal or mesh structures are considered in [13]. In a real situation, it may not be feasible to place BSs in a hexagonal or mesh structure. This paper considers the networks with an irregular structure and presents an algorithm to determine the positioning accuracy of the cell-based method in irregular networks. The positioning accuracy of the cell-based method

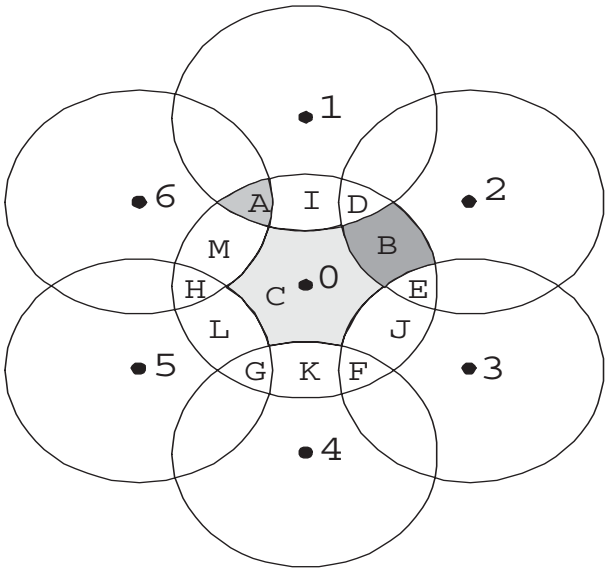
is dependent on the separation distance between two adjacent BSs and the transmission ranges of these BSs. Determining the optimal transmission range is a combinatorial optimization problem. Given a set of BS i, $i = 1, \ldots, n$, each with a fixed location and its transmission range $r_i, a \leq r_i \leq b$, we want to find a set of transmission ranges $(r_1^*, r_2^*, \ldots, r_n^*)$ such that the positioning accuracy is optimal. This is a difficult combinatorial problem. In this paper, we present a simulated annealing (SA) [17-22] algorithm to solve it because SA can provide an approximate solution for difficult optimization problems in reasonable time. SA was proposed by Kirkpatrick, Gelatt and Vecchi [17], who reported promising results based on numerical experiments. Since then there has been many papers on the topic. For detailed descriptions of SA, one can refer to a survey paper by Collins, Eglese and Golden [22].

Our simulation results show that 1) the accuracy can be improved up to 30% by SA; 2) the accuracy increases if the number of BSs increases; however, after a threshold the accuracy improvement is not noticeable; and 3) if we can place the BSs in an appropriate place, better accuracy can be achieved. After allocating BSs to optimal places, adjusting transmission ranges of BSs gives little contribution to improving accuracy.

The remainder of this paper is organized as follows. Section 2 presents the cell-based positioning method and its application. Section 3 gives the positioning accuracy of networks. The improved accuracy with power adjustment and simulation results are shown in Section 4. Finally, the conclusions are given in Section 5.

2 Cell-based positioning method and its application

Consider a physical layout of a wireless network as shown in Fig. 1. The area covered by the BS is called a *cell* and each cell is circle-shaped. That is, one assumes a perfectly spherical radio propagation for this idealized model. The



Regions	BSs Id
A	0, 1, 6
B	0, 2
C	0
D	0, 1, 2
E	0, 2, 3
F	0, 3, 4
G	0, 4, 5
H	0, 5, 6
I	0, 1
J	0, 3
K	0, 4
L	0, 5
M	0, 6

Figure 1: A layout of the wireless network.

signal coverage of the base stations may overlap. The mobile station (MS) can receive radio signals containing the base stations' IDs, if the identifier is within the signal coverage of that BS. For example, as shown in Fig. 1, an MS in region A can listen to signals from BSs 0, 1 and 6; in region B, from BSs 0 and 2; and in region C, from BS 0. We define a localization region as one in which every MS in the region receives a unique set of base stations' signals. As shown in Fig. 1, the coverage of BS 0 has 13 localization regions, i.e., all the regions from A to M.

Suppose one has a location server in the network maintaining a table in which a set of BS ID is bound to certain localization regions. When an MS reports to the location server that it can receive the signals from base stations 0, 1 and 6, the location server looks up the binding table and determines that the MS is in region A. One can thus determine the MS's location. This method is known as the cell-based positioning method, the topic of this paper.

In the following, we illustrate how to deliver location-based services by applying cell-based positioning method. Fig. 2 shows an architecture of the location-based service system. This system includes a central delivery platform and three servers, content server, location server, and Geographical Information System (GIS) server.

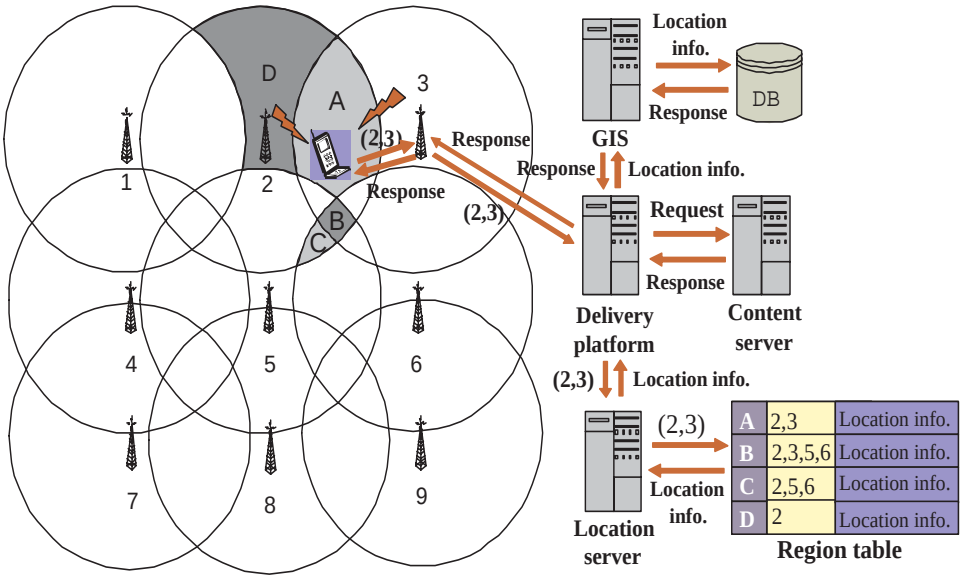


Figure 2: An architecture of the location-based service system.

The delivery platform integrates the servers to deliver mobile location-based services. The content server provides the relevant content, services and applications. The location server maintains the signal coverage of base stations and determines the location of mobile user. The GIS server provides the map and geographical information. As shown in Fig. 2, an MS in region A can listen to the signals from BSs 2 and 3. Then, the MS sends the location-based service request with cell ID (2, 3) to the delivery platform via BS 3. The delivery platform queries the MS's location by sending cell ID (2, 3) to location server. The location server looks up the region table and returns the MS's location to the delivery platform. Then, based on the MS's location, the delivery platform obtains the local information from GIS server and the relevant content from content server. Finally, the delivery platform prepares the requested service and replies it to the MS.

Note that the accuracy of the cell-based positioning method can be defined as the size of the localization region. The maximum of all localization regions is the location-sensing accuracy of the given network. As the localization regions become smaller, then the location-sensing accuracy improves.

3 Positioning accuracy of networks

This section considers a wireless network with n BSs in which the location of BS_i, (x_i, y_i) and its transmission range, r_i, are given where $i = 1, 2, ..., n$. The radio coverage of BS_i is denoted as circle C_i. By using simple geometry, we can find all the intersections of all the circles. Then, we can formulate the positioning accuracy problem into a *geometry graph model* $G = (V, E)$. Each vertex in set V stands for intersection points of C_i and C_j, and an arc (u, v) is in E if (u, v) is a simple segment of the circle where a simple segment means there is no intersection point between u and v. We called a vertex v as a border vertex if v is not inside another circle. An arc (u, v) is called a border arc if both u and v are border vertices. For example, a wireless network as shown in Fig. 3 can be represented by the graph $G = (V, E)$, where $V = \{v_1, v_2, \ldots, v_6\}$ and $E = \{(v_1, v_2), (v_2, v_3), (v_3, v_4), (v_4, v_1), \ldots, (v_5, v_4), \ldots, (v_2, v_5)\}$. Vertices v_1, v_4 and v_5 are border vertices and arcs $(v_1, v_4), (v_4, v_5)$ and (v_5, v_1) are border arcs. Note that the localization region R_1 is bounded by a set of arcs $(v_1, v_2), (v_2, v_6), (v_6, v_1)$. Thus, the problem of finding the accuracy for the cell-based positioning method is equivalent to finding the maximum size of a localization region in the graph $G = (V, E)$. An algorithm is presented below for finding all localization regions of G and calculating their areas. Therefore, the maximum size of a localization region can be determined.

3.1 Localization region finding algorithm

Let $Adj[u]$ denote the adjacency list of u. That is, $Adj[u]$ consists of all the vertices adjacent to u in G. For two vertices $v_1, v_2 \in Adj[u]$, we define angle $\angle v_1 u v_2$ to be the angle from arc (v_1, u) to arc (v_2, u) in a counter-clockwise direction. A cycle $P_i = (v_{i_1}, v_{i_2}), \ldots, (v_{i_k}, v_{i_1})$ is called a *simple cycle* if it forms a localization region. A simple cycle can be found by the following search procedure. Start to search from any arc (u, v) and set $P_i = (u, v)$. The following arc $(v, v_{j_1^*})$, $v_{j_1^*} \in Adj[v] \backslash \{u\}$,

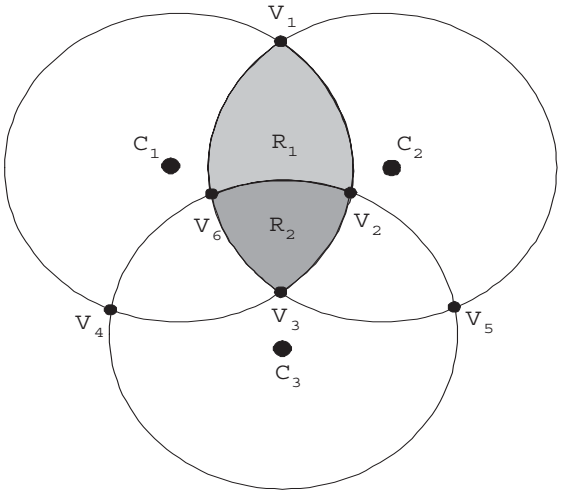


Figure 3: A geometry graph G.

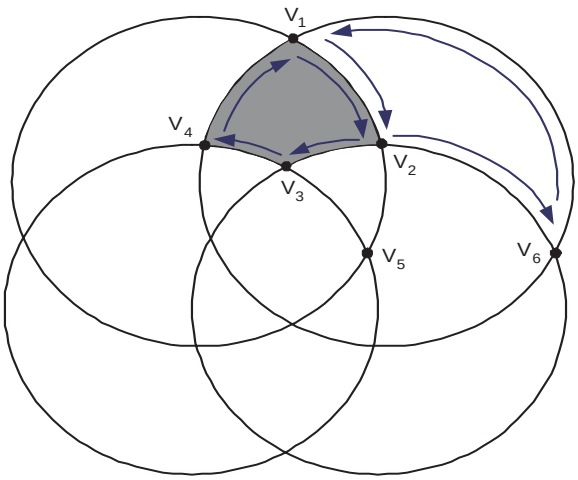


Figure 4: A simple cycle search in clockwise direction.

can be chosen into P_i is the arc with minimum angle $\angle uvv_{j_1^*}$. (i.e., $\angle uvv_{j_1^*} = \min_{v_{j_1} \in Adj[v] \setminus \{u\}} \angle uvv_{j_1}$). Now, $P_i = (u, v), (v, v_{j_1^*})$. Next, consider arc $(v, v_{j_1^*})$ and find the following arc $(v_{j_1^*}, v_{j_2^*})$ for P_i such that $\angle vv_{j_1^*}v_{j_2^*} = \min_{v_{j_2} \in Adj[v] \setminus \{u\}} \angle vv_{j_1^*}v_{j_2}$. Repeat the same procedure until the vertex u is reached. Then, a simple cycle $P_i = (u, v), (v, v_{j_1^*}), \ldots, (v_k^*, u)$ is found. For example, as shown in Fig. 4, start from (v_1, v_2). The next arc selected is (v_2, v_3). This is because $\angle v_1v_2v_3 < \angle v_1v_2v_5 < \angle v_1v_2v_6$. Similarly, choose (v_3, v_4) as the next arc of (v_2, v_3). By this way, a simple cycle $(v_1, v_2), (v_2, v_3), (v_3, v_4), (v_4, v_1)$ is found.

Note that such a simple cycle found is in a clockwise direction relative to arc

(u, v). Similarly, we can also find another simple cycle for (u, v) in a counter-clockwise direction. This can be done by selecting the next arc $(v, v_{i_1^*})$ of (u, v) such that $\angle uvv_{i_1^*} = \max_{v_{i_1} \in Adj[v] \setminus \{u\}} \angle uvv_{i_1})$. Repeat this procedure until the vertex u is reached. For example, simple cycle $(v_1, v_2), (v_2, v_6), (v_6, v_1)$ was found by a counter-clockwise search.

Suppose that for a given graph G, it has ℓ simple cycles. Let $P_i = (v_{i_1}, v_{i_2}), \ldots,$ $(v_{i_k}, v_{i_1}), i = 1, ..., \ell$ denote all simple cycles in G. Observing these cycles, we found that for any arcs (v_i, v_j) if they are not border arcs, there are two cycles P_s and P_t containing it; otherwise only one cycle P_u contains it. Thus, we can maintain data structures $counter[(u, v)]$ and $region[(u, v)]$ for each arc (u, v). If (u, v) is not a border arc, $counter[(u, v)]$ is set to 2; otherwise, $counter[(u, v)] = 1$. The $region[(u, v)]$ is a set consists of the localization regions separated by (u, v). For example, if (u, v) separates regions i and j, then $region[(u, v)] = \{i, j\}$.

The main idea behind the region finding algorithm is that we search each cycle i, $P_i = (v_{i_1}, v_{i_2}), \ldots, (v_{i_k}, v_{i_1})$, to see which forms localization region i. Then, for each arc (u, v) in P_i, set $counter[(u, v)] = counter[(u, v)] - 1$ and $region[(u, v)] = region[(u, v)] \cup \{i\}$. Note that if all counters of the arcs become zero, then all localization regions are found.

A brief pseudocode for the region finding is given as follows.

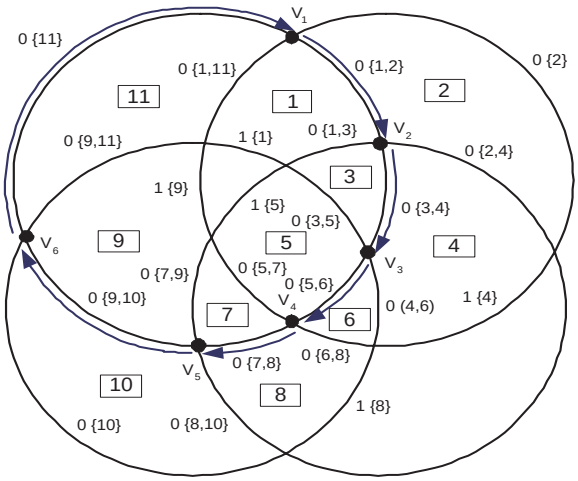


Figure 5: An example of region finding.

```
0   Procedure LRSEARCH(G = (V, E))
1     RegionNumber = 0
2     for all (u, v) ∈ E do
3       region[(u, v)] = ∅
4       if (u, v) is not a border arc then counter[(u, v)] = 2
5          else counter[(u, v)] = 1
6     for all (u, v) ∈ E do
7       while counter[(u, v)] ≠ 0 do
8       begin
9         if counter[(u, v)] = 1 and region[(v, u)] ⊆ region[(u, w)]
10           then find a simple cycle in counterclockwise direction, say P_i
11           else find a simple cycle in clockwise direction, say P_i
12           (comment: w ∈ Adj[u] with ∠uvw = min_{v_j ∈ Adj[v]\{u}} ∠uvv_j)
13        RegionNumber = RegionNumber + 1
14        for all (u_i, v_i) ∈ P_i do
15           counter[(u_i, v_i)] = counter[(u_i, v_i)] − 1
16           region[(u_i, v_i)] = region[(u_i, v_i)] ∪ {RegionNumber}
17      end
18    return(region[(u, v)])
```

An example to illustrate the above procedure is given in Fig. 5. After applying lines 7 to 17 of Procedure LRSEARCH to arcs, $(v_1, v_2), (v_2, v_3)(v_3, v_4)(v_4, v_5)(v_5, v_6)$ and (v_6, v_1), the 11 localization regions are found as shown in Fig. 5. (Note that 13 localization regions will be found after all arcs are considered.) Values in the square represent region number and values along the arcs represent $counter[u, v]$ and $region[(u, v)]$.

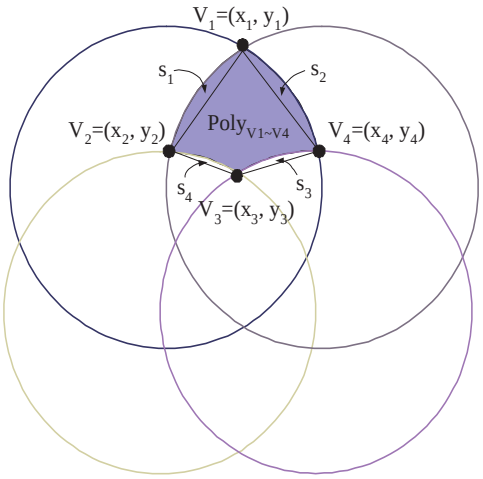


Figure 6: The component of a circle area.

3.2 Area of the localization region

Consider a localization region R_1 which is formed by simple cycle $(v_1, v_2), (v_2, v_3), (v_3, v_4), (v_4, v_1)$ in Fig. 6. Note that region R_1 includes polygon $v_1v_2v_3v_4$ and bow segments S_1 and S_2, and excludes bow segments S_3 and S_4. Let $g_{v_1 \ldots v_k}$ denote polygon $v_1 \ldots v_k$ and $s(X)$ denote area of X. Then, the area of localization region $(v_1, v_2), (v_2, v_3), (v_3, v_4), (v_4, v_1)$ is equal to $s(g_{v_1v_2v_3v_4}) + s(S_1) + s(S_2) - s(S_3) - s(S_4)$. In general, if localization region R_i includes polygon $g_{v_1, v_2, \ldots v_k}$ and bow segments $S_1, \ldots, S_a$, and excludes $S_{a+1}, \ldots, S_k$, then the area of the region is

$$s(R_i) = s(g_{v_1 \ldots v_k}) + (\sum_{i=1}^{a} s(S_i)) - (\sum_{i=a+1}^{k} s(S_i))$$

The areas of polygon and bow segments can be found as follows.

1) The area of polygons

The area of a polygon can be calculated by a cross product formula [23] in the counter-clockwise order of vertices. That is, if the coordinates of polygon $g_{v_1 \ldots v_n}$ are (x_1, y_1),...,(x_n, y_n), then the area of polygon $g_{v_1 \ldots v_n}$ can be determined by

$$s(g_{v_1 \ldots v_n}) = \frac{1}{2} \sum_{k=1}^{n} \begin{vmatrix} x_k & x_{k+1} \\ y_k & y_{k+1} \end{vmatrix}$$

where $x_{n+1} = x_1,\ y_{n+1} = y_1$.

2) The area of bow segments

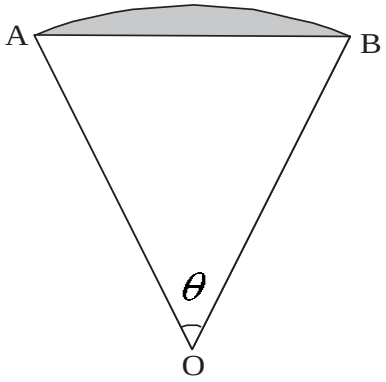


Figure 7: The area of a bow segment.

The area of bow segment S_i, as shown in Fig. 7, can be calculated by

$$\begin{aligned} s(S_i) &= \frac{1}{2}\theta\ r^2 - s(\triangle_{AOB}) \\ &= \frac{1}{2}\theta\ r^2 - \frac{1}{2}[2r^2 \sin(\frac{\theta}{2})\cos(\frac{\theta}{2})] \end{aligned}$$

where r is the transmission range of the cell and $\theta = \angle AOB$.

Suppose that we found ℓ localization regions by using a region finding algorithm and evaluated each area of region R_i. Then, the accuracy $e(r_1, r_2, \ldots, r_n)$ of the cell-based positioning method can be obtained by:

$$e(r_1, r_2, \ldots, r_n) = \max_{1 \le i \le \ell}\{R_i\} \tag{1}$$

where r_i is transmission range of BS $i, 1 \le i \le n$.

4 Improving accuracy with power adjustment

If the transmitting power of the BS can be adjusted, then the coverage of the BS varies. Consider the problem that given a set of BS i, $i = 1, \ldots, n$, with a fixed location and its transmission range $r_i, a \le r_i \le b$, we want to find a set of transmission ranges $(r_1^*, r_2^*, \ldots, r_n^*)$ such that the positioning accuracy is optimized. This problem is equivalent to finding a set of transmission ranges $(r_1^*, r_2^*, \ldots, r_n^*)$ such that $e(r_1, r_2, \ldots, r_n) = \max_{1 \le i \le \ell}\{R_i\}$ is minimized. That is,

$$z(r_1^*, r_2^*, \ldots, r_n^*) = \min_{(r_1, r_2, \ldots, r_n)} e(r_1, r_2, \ldots, r_n)$$

where $a \leq r_i \leq b,\ i = 1, 2, \ldots, n$.

In this section, we applied Simulated Annealing (SA) to solve this optimization problem.

1) Simulated annealing

Recently, SA has become more popular for solving large-scale combinatorial optimization problems with approximate optimization solutions. The advantage of SA is that it provides a general purpose solution for a wide variety of combinatorial optimization problems. Thus, SA is used in many fields such as computer-aided design of integrated circuits, image processing, code-designed, neural network theory and so on.

In general, the SA algorithm is similar to metal-cooling. During slow cooling, a metal rearranges the atoms into regular crystalline structures with high density and low energy. The SA algorithm starts with an initial solution $s_0 = (r_1^0, r_2^0, \ldots, r_n^0)$, and finds the value of cost function $e(s_0) = e(r_1^0, r_2^0, \ldots, r_n^0)$, also known as *fitness function*(see equation (1)). Let s_i be the current solution with cost function $e(s_i)$. For each iteration j, generate a random neighbor s_j of s_i and evaluate its cost function $e(s_j)$. If $e(s_j) \leq e(s_i)$, then s_j is accepted (i.e., set $s_i = s_j$ and $e(s_i) = e(s_j)$). Otherwise, the s_j will be accepted with the probability $p = \min\{1, \exp((e(s_i) - e(s_j))/T)\}$. The parameter of T means the "temperature" which changed with parameter α for each iteration. This is known as the Metropolis criteria [18] and the pseudocode is shown below:

Step 1: Initialize the temperature T. Generate an initial solution s_0 and set current solution $s_i = s_0$.

Step 2: Generate a trial solution s_j, a random neighbor of s_i.

Step 3: Let $\triangle e = e(s_j) - e(s_i)$.

Step 4: If $\triangle e \leq 0$, then the trial solution s_j is accepted. Set current solution $s_i = s_j$

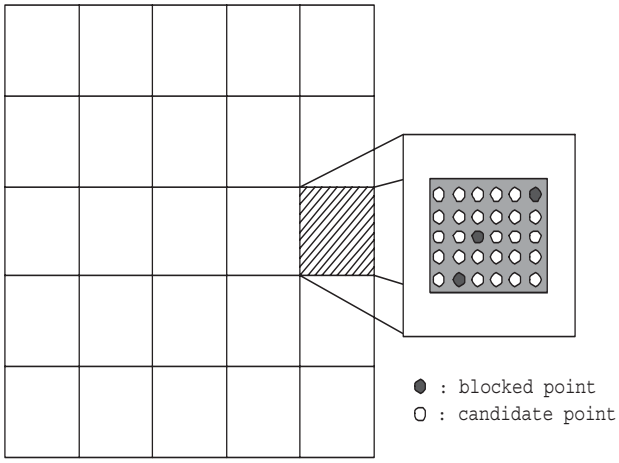


Figure 8: Grid-based deployment.

and $e(s_i) = e(s_j)$.

If $\triangle e > 0$, then the trial solution s_j is accepted with the probability $p = \exp(\frac{-\triangle e}{T}) > d$, where d is a random number in $[0, 1]$. Set current solution $s_i = s_j$ and $e(s_i) = e(s_j)$.

Otherwise, go to Step 2.

Step 5: Repeat Steps 2-4 for I_t iterations.

Step 6: $T = T \times \alpha$.

Step 7: Repeat Steps 2-6, until $T < T_{stable}$.

In this simulation, we set $I_t = 300, T = 1, T_{stable} = 0.05$ and $\alpha = 0.85$.

2) Simulation results

This simulation ran on networks of $25, 36, 49, \ldots, 225$ BSs in a square service area of 500 units $\times$ 500 units, respectively. We divided the service area into n grids (see Fig. 8) where n is the number of BSs. As shown in Fig. 8, white points, called candidate points, represent possible locations to place a BS in the grid. The black points represent block points where one cannot place a BS. Assume that the signal of the BS must cover the entire grid.

Four types of adjustments are considered for improving the accuracy of the cell-based positioning method.

Type 1: Assume that the locations of BSs are given and the transmission ranges of the BSs are identical. We evaluate $e(r, r, \ldots, r)$ for $r = a, a+\delta, \ldots, a+k\delta$ where $k = \lfloor \frac{0.6a}{\delta} \rfloor$ and a is a minimal transmission range such that entire service area is covered. Then find $z(r^*, r^*, \ldots, r^*) = \min\{e(r, r, \ldots, r) | r = a, a+\delta, \ldots, a+\lfloor \frac{0.6a}{\delta} \rfloor \delta\}$. (In our simulation, we set $\delta = 1$.)

Type 2: Assume that the locations of BSs are given and the transmission ranges $r_i, i = 1, 2, \ldots, n$, are in $[a, 1.6a]$. The SA is applied to the network to find a set of transmission ranges $(r_1^*, r_2^*, \ldots, r_n^*)$ such that $z(r_1^*, r_2^*, \ldots, r_n^*) \approx \min_{(r_1, r_2, \ldots, r_n)} e(r_1, r_2, \ldots, r_n)$.

Type 3: Assume that the transmission ranges $r_i, i = 1, 2, \ldots, n$, of the BSs are given. SA is applied to the network to allocate the locations (x_i, y_i) of BSs such that $z(r_1, r_2, \ldots, r_n) \approx \min_{(x_1, y_1), \ldots, (x_n, y_n)} e(r_1, r_2, \ldots, r_n)$ where (x_i, y_i) is the coordination of BS i.

Type 4: This is a combination of Types 2 and 3. For a given $(r_1, r_2, \ldots, r_n)$, SA is applied to allocate the locations of BSs. Then, use SA again to adjust transmission ranges $r_i, i = 1, 2, \ldots, n$, of the BSs.

Because the optimal value of $z(r_1^*, r_2^*, \ldots, r_n^*)$ is hard to find, we use a lower bound of $z(r_1^*, r_2^*, \ldots, r_n^*)$, denoted as LB, for comparison. A lower bound of $z(r_1^*, r_2^*, \ldots, r_n^*)$ is obtained as follows. By simulation, we can estimate the maximum number of localization regions for each network. Then, the whole service area divided by the maximum number of localization regions can be used as a lower bound of $z(r_1^*, r_2^*, \ldots, r_n^*)$. Table 1 summarizes the maximum number of localization regions and the lower bound of $z(r_1^*, r_2^*, \ldots, r_n^*)$ for each network.

Table 1. The maximum number of regions and LBs of $z(r_1^*, r_2^*, \ldots, r_n^*)$.

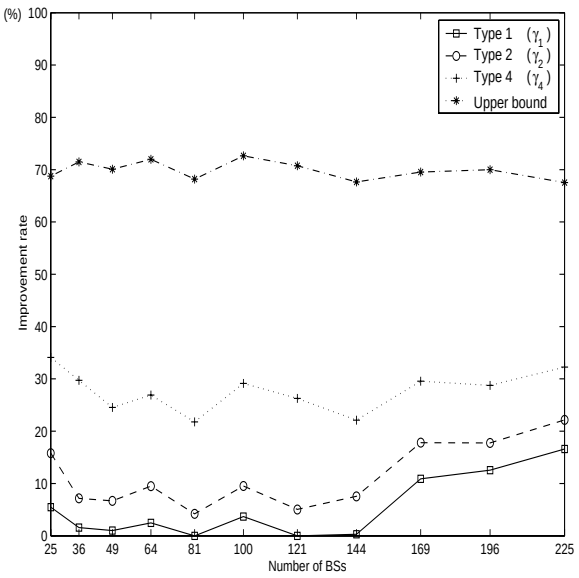


Figure 9: The improvement rates of Types 1, 2, and 4, and the upper bound.

Number of BSs in the network	25	36	49	64	81	100	121	144	169	196	255
Maximum region number	168	246	325	416	499	601	673	739	798	865	893
LB of $z(r_1^*, r_2^*, \ldots, r_n^*)$	1488	1016	769	601	501	416	371	338	313	289	280

In order to show the performance of the proposed methods, comparisons between the accuracy after the adjustments and the accuracy before the adjustment are made. Let Z_i denote the accuracy $z(r_1^*, r_2^*, \ldots, r_n^*)$ found by Type i and Z_0 denote the initial accuracy $e(r_1^0, r_2^0, \ldots, r_n^0)$ where $(r_1^0, r_2^0, \ldots, r_n^0)$ is an initial solution. Fig. 9 shows the improvement rate γ_i of Type $i, i = 1, 2, 4$ where the improvement rate $\gamma_i = \frac{|Z_i - Z_0|}{Z_0} \times 100\%$. Besides, an upper bound of improvement rate $\bar{\gamma}^* = \frac{|LB - Z_0|}{Z_0} \times 100\%$ is also shown in Fig. 9. From Fig. 9, note that the accuracy can be improved up to 30% by the Type 4 method.

Fig. 10 shows the relationships between the accuracy and the number of BSs in the network. The y-axis is the normalized accuracy defined as the percentage of the localization area compared to the entire service area. For example, the normalized accuracy of the lower bound is $\frac{338}{250000} \times 100\% = 0.14\%$ for the network with 144 BSs. From Fig. 10, we learned that increasing the number of BSs from

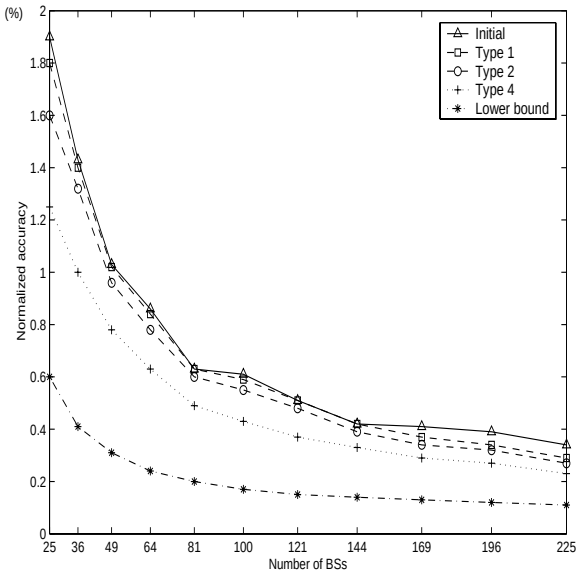


Figure 10: The relationships between the accuracy and the number of BSs in the network.

25 to 144, the accuracy is improved greatly. However, when the number of BSs is more than 144, the improvement of accuracy is insignificant.

Finally, the improvement rates of accuracy of Types 3 and 4 are compared in Fig. 11. The results of the two types are almost the same. This means that for accuracy, the factor of allocating the BSs' locations is more significant than the factor of adjusting transmission ranges. If we can place the BSs in appropriate places, the accuracy of cell-based positioning method will be better.

5 Conclusions

This paper presented an algorithm to determine the positioning accuracy of the cell-based method for networks with irregular structures. Because the positioning accuracy of the cell-based method is dependent on the separation distance between two adjacent BSs and the transmission ranges of these BSs, we proposed a SA method to determine the locations and transmission ranges of BSs in order to achieve a better positioning accuracy. Our simulation results showed that the accuracy can be improved up to 30% by the proposed method.

The main advantage of cell-based method is that it requires no changes to the

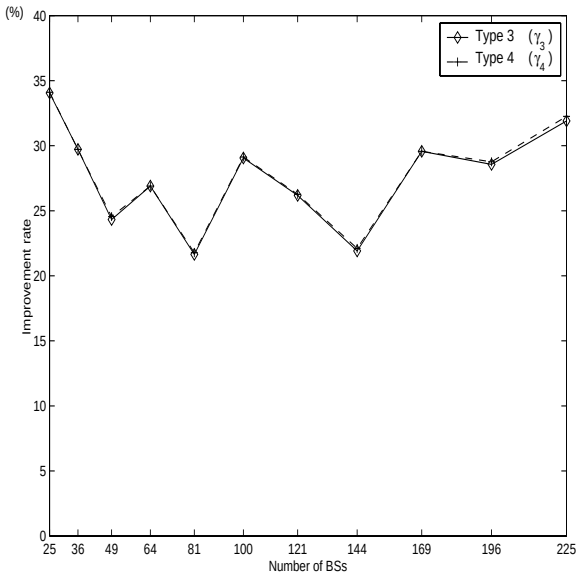


Figure 11: The improvement rates of Types 3 and 4.

existing network architecture, or to the handset. It only requires several lines of code on the SIM card to get the list of BSs. Thus, it does not substantially increase costs for either network operators or end users. The accuracy of cell-based positioning increases as the number of cells within range increases. Therefore, the cell-based method functions best in urban.

However, the proposed cell-based method is restricted in the idealized radio model, i.e., we assume the perfect spherical radio propagation in the idealized radio model. In fact, the coverage of a BS is not necessarily a circle. In most cases, it is location-dependent and probably irregular. The positioning problem with a more realistic radio model might be interesting for possible future work. The following cases are the most interesting:

1. Non-circular coverage: The coverage of a BS may not be circular. For example, in the real world, the BSs may have 1, 2, 3, or 6 sectors. Besides, the terrain can produce irregular coverage area. Our cell-based method might be extended to solve the positioning problem with irregular coverage, under the condition that each BS's coverage can be precisely defined and no two localization regions receive the same set of BS signals.

2. Multiple power levels: BSs can be of Macrocell, Microcell and Picocell types and have variable power. Or, BSs can transmit beacon signals with multiple power levels. In such cases, the better positioning accuracy can be achieved. We are currently working on these extensions, and the results will be reported in our future papers.

3. Noisy environments: Noisy environments are characterized by severe multi-path phenomenon, fading, obstructions, etc. Adapting the cell-based method to noisy environments is also our future work.

In addition to relax the idealized radio model, other measures of accuracy are interesting for possible future work. For example, the worst case of accuracy error can be defined as the diameter of the region. Evaluating the worst case accuracy should be interesting and useful.

References

[1] N. Davies, K. Cheverst, K. Mitchell, and A. Efrat, "Using and determining location in a context-sensitive tour guide", *IEEE Computer Magazine*, vol. 34, pp. 35-41, Aug. 2001.

[2] K. Chadha, "The global positioning system: challenges in bringing GPS to mainstream consumers", *In IEEE International Solid-State Circuits Conference*, pp. 26-28, 1998.

[3] A. Marsh, M. May, and M. Saarelainen, "Pharos: coupling GSM and GPS-TALK technologies to provide orientation, navigation and location-based services for the blind", *In Proc. of IEEE EMBS International Conference on Information Technology Applications in Biomedicine*, pp. 38-43, 2000.

[4] G. M. Djuknic, and R. E. Richton, "Geolocation and assisted GPS", *Computer Magazine*, vol. 34, pp. 123-125, Feb. 2001.

[5] E. Kotsakis, A. Caignault, W. Woehler, and M. Ketselidis, "Integrating differential GPS data into an embedded GIS and its application to infomobility and navigation", *In Proc. of the 7th EC-GI and GIS Workshop EGII-Managing the Mosaic*, Jun. 2001.

[6] G. J. Morgan-Owen, and G. T. Johnston, "Differential GPS positioning", *Electronics and Communication Engineering Journal*, vol. 7, pp. 11-21, Feb. 1995.

[7] J. C. Jubin, and D. L. Shaver, "Wide-area differential GPS reference-station placement", *Position Location and Navigation Symposium*, pp. 503-514, 1996.

[8] C. Drane, M. Macnaughtan, and C. Scott, "Positioning GSM telephones," *IEEE Communications Magazine*, vol. 36, pp. 46-54, Apr. 1998.

[9] J. M. Zagami, S. A. Parl, J. J. Bussgang, and K. D. Melillo, "Providing universal location services using a wireless E911 location network", *IEEE Communications Magazine*, vol. 36, pp. 66-71, Apr. 1998.

[10] T. S. Tappaport, J. H. Reed and B. H. Woerner, "Position location using wireless communications on highways of the future", *IEEE Communication Magazine*, vol. 34, pp. 33-34, 1996.

[11] L. Doherty, K. S. J. Pister, and L. E. Ghaoui, "Convex position estimation in wireless sensor networks," *In Proc. of INFOCOM*, vol. 3, pp. 1655-1663, 2001.

[12] C. Drane, M. Macnaughtan, and C. Scott, "The accurate location of mobile telephones," *In 3rd World Conf. on Intelligent Transport Sys.*, Oct. 1996.

[13] H.-C. Chu and R.-H. Jan, "A Cell-Based location-sensing method for wireless networks", *Wireless Communication and Mobile Computing*, vol. 3, pp. 455-463, 2003.

[14] S. Meguerdichian, F. Koushanfar, M.Potkonjak, and M. B. Srivastava, "Coverage problems in wireless ad-hoc sensor networks", *In Proc. of IEEE INFOCOM*, vol. 3, pp. 1380-1387, 2001.

[15] S. L. Wu, Y. C. Tseng, and J. P. Sheu, "Intelligent medium access for mobile ad hoc networks with busy tones and power control", *In Proc. of 8th International Conference on Computer Communications and Networks*, pp. 71-76, 1999.

[16] C. F. Huang, Y. C. Tseng, S. L. Wu, and J. P. Sheu, "Increasing the throughput of multihop packet radio networks with power adjustment", *In Proc. of 10th International Conference on Computer Communications and Networks*, pp. 220-225, 2001.

[17] S. Kirkpatrick, C. D. Gelatt, Jr., and M. P. Vecchi, "Optimization by simulated annealing", *Science*, vol. 220, no. 4598, pp. 672-680, May 1983.

[18] P. J. M. van Laarhoven and E. H. L. Aarts, "Simulated annealing: theory and applications", Dordrecht, D. Reidel, 1987.

[19] D. S. Johnson, C. R. Aragon, L. A. McGeoch and C. Schevon,"Optimization by simulated annealing: an experimental evaluation; part II, graph coloring and number partitioning", *Operations Research*, vol. 39, pp. 378-406, 1991.

[20] A. H. Mantawy, Y. L. Abdel-Magid, and S. Z. Selim,"A simulated annealing algorithm for unit commitment", *IEEE Transactions on Power Systems*, vol. 13, pp. 197-204, Feb. 1998.

[21] A. Y. Zomaya, "Natural and simulated annealing", *Computing in Science and Engineering*, vol. 3, pp. 97-99, Nov.-Dec. 2001.

[22] N. E. Collins, R. W. Eglese, and B. L. Golden, "Simulated annealing: an annotated bibliography", *American Journal of Mathematical and Management Sciences*, vol. 8, pp. 209-307, Jan. 1988.

[23] G. B. Thomas and R. L. Finney, "Calculus and analytic geometry", 9th edition, Addison-Wesley, Jun. 1998.