# 以誠信機制代理人中介之行動隨意網服務探尋與選擇

何偉碩
國立嘉義大學資工系
oure3g@yahoo.com.tw

陳志翔
國立嘉義大學資工系
stanly.chen@msa.hinet.net

徐超明
國立嘉義大學資工系
rchsu@mail.ncyu.edu.tw

## 摘要

本文探討在行動隨意網路（Mobile Ad-hoc Network, MANET）環境下利用代理人（Agent）技術之 Contract Net 協定幫助使用者透過代理人溝通協商的行為完成服務探尋（Discovery）與選擇（Selection）。本研究利用兩階段（2-phase）方式進行服務探尋，第一階段是利用代理人溝通協商協定之 Contract Net Protocol（CNP）以混合 Push Model 與 Pull Model 方式進行 MANET 環境下之服務探尋；第二階段則改善傳統 CNP 的不足之處，使用 Extended Contract Net Protocol（ECNP）以訂定動態簽訂服務合約的動作進行，並於 ECNP 其中加入模糊認知圖（Fuzzy Cognitive Map）進行代理人誠信（Trust）計算，除了讓代理人能在服務效率不如預期或出現惡意行為時進行判斷程序以選擇最適合使用者的服務，並同時能提升服務探尋機制的效率。本研究所提出的架構並經程式模擬分析驗證確認其成效。

**關鍵詞**：Service Discovery, Service Selection, Fuzzy Cognitive Map, MANET。

## 1. 前言

不同於路由協定，服務探尋（Service Discovery）位於較高的應用層，用來管理、分享及尋找需要的資源，這些資源可能是指令、檔案，甚至是軟硬體的使用。利用服務探尋機制，能夠以資源分享的概念，讓原本不具備某種功能的機器完成之先無法做到的任務。目前存在一些可以找到遠端服務的尋找機制，例如 IETF 的 Service Location Protocol（SLP）[10]、SUN Jini[17]、及 Microsoft UPnP[14]，這些機制皆為針對有線網路環境設計，大多必須有一個中央註冊伺服器來管理整個環境，而 Bluetooth SDP[22]雖是屬於無線隨意網中對具有 Bluetooth 硬體設備的探尋，但仍需要有集中管理角色的存在。然而在 MANET 中，每個新加入的裝置必須知道區域內存在的服務，以及公佈自己所能提供的服務，或是在離開時能通知其他裝置服務即將停止，這些動作都需要使用廣播（broadcast）或群播（multicast）訊息來傳遞給區域內的裝置。但是大量的廣播不只會耗費頻寬，也容易造成碰撞的發生，導致訊息必須重傳，間接消耗額外的能量。因此，必須要設計一個能夠適用於 MANET 環境下，良好的服務探尋機制，並在效能（如正確率、服務成功率）及耗費（如訊息傳送量）中取得平衡。

另外，在服務探尋機制研究中，許多都是預設網路環境內的裝置皆為誠實可靠、不會提供錯誤或惡意的資料。但實際的網路裡，可能會有裝置運算能力不足、傳輸效率不佳，甚至惡意使用者將病毒或木馬偽裝成正常程式提供出去，而一無所知的服務尋找協定卻將其公佈在網路環境中，如此一來不僅使得網路利用度不佳，甚至會影響整個網路內的裝置受害，服務尋找機制就變的沒有效率且不可靠。因此基於這個問題，本研究加入一套實用的『誠信（Trust）』機制，建立行動裝置的名聲（Reputation），有效的維持整個服務探尋的正確性、安全性，及早遏止惡意使用者或不良裝置進行破壞行為。

## 2. 相關文獻探討

服務探尋機制是要讓服務要求端（Service Requester）找到提供者端（Service Provider）所提供的服務，這些服務可以定義成硬體的共用，例如印表機、傳真機、攝影機的使用，也可以定義成軟體資訊的共享，例如影音多媒體串流服務或檔案下載、交通與天氣資訊回報或是當地旅遊景點與地圖顯示等相關訊息的取得。一般而言服務探尋機制的架構有『服務描述（service description）』、『服務廣告（service advertising）』、『服務尋找（service discovery）』和『服務傳送（service delivery）』幾項[6]，當服務提供者提供服務時，必須對此服務進行描述，才能讓其他人知道這項服務的功能；當一項服務完成描述，要讓其他人可以使用時，就必須對這個服務進行廣告，讓其他人得知服務的存在及位置；或是當某個人需要服務時，則可發送廣播或群播訊息尋找需要的服務，再讓可以提供服務的裝置使用單播（unicast）連結到要求者端；最後某兩部裝置溝通完成，就開始進行服務資料的傳送，達成服務探尋所需要的動作。

### 2.1 MANET 下的服務探尋

由於 Jini 的檢視伺服器（Lookup Server）、UPnP 的控制點（Control Point）、SLP 的目錄代理人（Directory Agent, DA）和藍芽的主裝置（Master）都是屬於集中式管理，並不適合用在 MANET 如此高移動、分散性、隨時都會改變網路組合的特性，

集中式的管理辦法對伺服器負擔太重且風險大，加上每個行動裝置都可能動態的加入或離開網路，維持這些資訊極為困難，因此必須要提供一個完全分散式的服務探尋機制，讓行動裝置在有限的資源下能發揮最大的功效。

目前在固定有線網路下進行服務探尋的研究已經被提出許多[21]，但都無法完全適用於 MANET 動態的環境下，因此設計一個合適於 MANET 的服務探尋機制是一個研究的重點。Kozat 和 Tassiulas 提出 Virtual Backbone[8][9]讓裝置可以尋找或註冊服務，環境中會存在中間人（Service Broker）扮演如 SLP 中目錄代理人的角色，讓一個範圍內的裝置可以對其進行服務尋找或註冊服務，這個方法適用於固定性高且範圍較小的 MANET 環境下。DEAPspace[15]為 IBM 實驗室 Nidd 所提出用於 MANET 環境下單點跳躍（single-hop）之服務探尋機制，這個方法是以分散式環境下使用 Push model 的概念所建立，在 DEAPspace 架構裡，每部裝置會使用一個快取記憶體（cache）儲存網路內所能提供的服務，而可以提供服務的裝置則會週期性的廣播廣告（advertisement）訊息，讓其他裝置知道服務的存在。其特點是每部裝置所儲存在快取內的廣告訊息也會週期性的廣播給附近裝置，如此一來能夠提升裝置找到服務的時間，讓服務探尋機制快速的完成。但是這個特點會因為廣播重複或不必要的訊息而大大的耗費頻寬，加上 MANET 動態加入或移出裝置，經常更新這些訊息是非常沒有效率的。有別於 DEAPSpace，Knoark[6][11] 綜合 Push model 和 Pull model 的概念，設計一個中介（middleware）架構，每部裝置能同時為服務提供者和服務要求者，並建立一個 micro-HTTP 伺服器處理接受到的要求訊息，而對於所暫存的廣告訊息則使用閒聊演算法（Gossip Algorithm），以群播的方式將要求訊息限制在鄰近裝置中，並與鄰近裝置交換暫存的廣告訊息，有效的將裝置所知的服務廣告傳播出去，減少大量重複的廣播訊息，因此在較大的 MANET 環境下顯得比較有效率。

## 2.2 誠信機制與 FCM

上述所提到的服務探尋協定，大多是預設在網路環境中所有裝置都具有足夠之資源（如運算能力、頻寬等），並且所有裝置都是善意、不會提供錯誤或惡意的資料。但實際的 MANET 裡，可能會有裝置運算能力不足、傳輸效率不佳，甚至惡意使用者將病毒或木馬偽裝成正常程式提供出去，而一無所知的服務探尋協定卻協助其公佈在網路環境中，如此一來不僅使得網路利用度不佳，甚至會影響整個網路內的裝置受害，服務探尋機制就變的沒有效率且不可靠。因此本研究建立一個具信任值參數計算的代理人機制，負責服務的提供、搜尋以及建構簡單的誠信機制。

誠信（Trust）機制常見於電子商務安全上[4]，又分為無信任第三者（Trusted-Third-Party）和有信任第三者[5]，前者因為不需要一個中央管理中心來掌控信任機制，所以適用於分散式 MANET 環境。利用誠信機制建立網路裝置的名聲（Reputation）[19]，能有效的維持整個服務探尋的正確性、安全性，及早遏止惡意程式或木馬進行破壞行為。關於信任值（trust value）的計算已有很多研究方法被提出，例如 Wang 和 Vassileva 提出 Bayesian Network-based Trust Model[20]，就是利用 Bayesian Network 計算信任參數，考慮一些環境中常見的變數，根據期間的因果關係統計代理人的名聲值；Aydin[3]等人利用簡單的二進位數值運算方法，有效的計算出由其他人所提供的檔案是否可以信任，甚至可以藉著延長紀錄的位元數，算出先前的互動中提供檔案的對方是否有不良或惡意的舉動，如此一來依據歷史的紀錄，更精準的決定該下載哪些檔案。Li 和 Ling[12]提出分散式點對點（peer to peer）環境的信任值計算，定義五個重要的參數( peer records, scope, credibility, transaction context, and community context）來評估其他裝置是否可以信任，並可用裝置之前服務的情況所得的名聲當作參考依據來計算，防止惡意使用者破壞電子商務安全。

所以本研究欲建構的誠信機制，除了能夠正確的算出信任值，還要能在環境參數遺失時也能正常工作。以認知（Cognitive）導向的信任計算正適合本研究所期望的情境，認知圖（Cognitive Map）是 1976 年由 Axelrod 所提出的理論[1]，主要目的是要解決非結構性問題，做出決策參考。認知圖的方法是建立一個網狀的因果圖建立點和點之間的因果關係，節點所代表的就是變數，而邊所代表的就是關係，根據這個因果圖可以計算變數之間的正負關係，並且可以描述其連鎖關係和影響，如下圖圖 1 即為一個簡單的認知圖模型，利用節點和邊來描述互相關係，經過計算後就能得知某個因素會因為某幾個因素變動而變動。

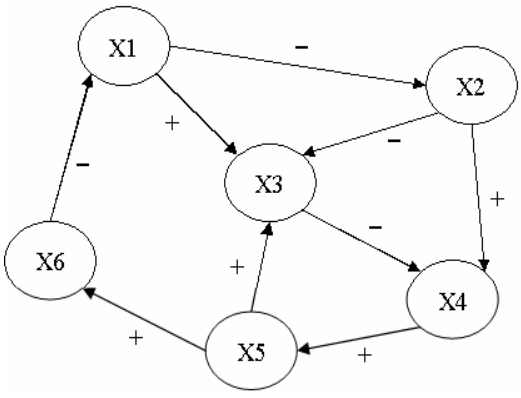


圖 1、Cognitive Map Network

模糊理論（fuzzy theory）的特點就是能將原本單純正負關係轉變成[-1,1]（根據不同門檻函數可以為-1~1 或 0~1 之間）的區間關係，所以當 Kosko 將

模糊理論套用到認知圖方法上成為模糊認知圖（Fuzzy Cognitive Map）[7]，就可以用來得知關係和關係間因果的『強度』，讓問題的答案解決後變的更有彈性且詳細，解決原始認知圖無法得知變數與變數間詳細的強度關係，還能在關係不明確或無法取得關係的狀況下照常推導，避免在傳統因果圖對於沒有界定或不明確定義下就無法工作的問題。在先前學者的研究中也曾經把 FCM 用來作為決策分析[16]或因果關係計算[13]，而 Ali 等人則利用 FCM 計算出信任值來尋找及選擇網頁服務（Web Service）[2][23]。因此 FCM 這個方法非常適合於本文欲提出的誠信機制之目標，讓本文所提出的代理人能夠以『模糊』的方式思考，建立類似於人類思考行為之架構。

## 3. 方法架構

本篇將架構分成服務探尋及服務選擇兩部分說明。第一階段為服務的要求尋找，利用額外儲存空間暫存服務廣告或提供者資訊，方便之後判斷選擇之用；第二階段為服務選擇，使用 FCM 計算可信任的服務提供者與之互動，並能在互動後根據服務的結果，當作之後繼續互動的經驗，或是提供給其他裝置作為名聲的考量。

### 3.1 第一階段-服務探尋

在服務探尋機制的第一階段，首先建立一個服務內容表（Service Content Map, SCM），SCM 的資料結構如圖 2 所示，儲存服務提供者資料及互動後經驗如圖 2（a），此 SCM 之內容記載某個服務（Service）由哪部提供者（Provider）所提供，和服務完成前根據評估所得到各裝置信任值（Computed Trust Value）以及服務完成後對某一特定裝置（如圖中 ID-3）之信任值評價（Assessed Trust Value），服務完成後的經驗值將可以提供給其他裝置作為名聲之用，而對沒有與其服務互動的提供者則不予紀錄（圖中以--表示）。SCM 之名聲值的暫存則如圖 2（b）所示，儲存推薦者（Recommending Device）所提供的某服務提供者之名聲，用於將來服務搜尋、評估與計算所用。一開始每部裝置進入 MANET 環境後，會以群播的方式將所能提供的服務發佈出去，讓其他裝置暫存於 SCM 中，發佈的廣告訊息內容為如服務的名稱、總類、描述和存活時間（Time-To-Live, TTL）等，以及附加的裝置能力描述（Speed, Quality, Cost 等），以用於之後的信任值計算，上述步驟即在於完成服務探尋中之 Push Model 的流程，將服務告知環境中其他裝置，之後除了服務更新之外，則不會再進行群播廣告訊息的動作，接下來即進入等待要求（Standby）的狀態。而當服務要求者（Service Requester）需要某個服務時，先從 SCM 中尋找相關資訊，若能找到則以點對點（point-to-point）方式直接向持有服務的提供者提出要求，而當服務要求者在 SCM 中找不到，或某個服務的存在無從得知時，則廣播要求訊息來詢問其他鄰近連網裝置，經由附近裝置協助來找到所需的服務。

| Service | Provider | Computed Trust Value | Assessed Trust Value | TTL |
|---|---|---|---|---|
| A1 | ID - 3 | 91 | 92 | 0957 |
| A1 | ID - 2 | 87 | -- | 0920 |
| A2 | ID - 3 | 85 | 87 | 0955 |
| A2 | ID - 1 | 75 | -- | 0920 |
| C2 | ID - 4 | 83 | 87 | 0935 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

（a）

| Service | Provider | Reputation | Recommending Device | TTL |
|---|---|---|---|---|
| A1 | ID - 3 | 85 | ID - 5 | 1000 |
| A1 | ID - 2 | 88 | ID - 7 | 1000 |
| A2 | ID - 3 | 89 | ID - 8 | 0955 |
| A2 | ID - 1 | 80 | ID - 4 | 0955 |
| A2 | ID - 3 | 73 | ID - 5 | 0955 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

（b）

圖 2、Service Content Map
（a）Trust Value Table （b）Reputation Table

本研究對於服務探尋機制採用 CNP[18]代理人溝通協定，以三個交握訊息作為服務要求的步驟，讓尋找服務的裝置由其他裝置取得所需要的服務或相關資訊，如圖 3 為服務要求步驟之示意圖。當裝置 1 要求 type a 的服務時，其鄰近有 ID 2、3 和 4 三部裝置，以及必須靠裝置 4 轉傳訊息的裝置 5 與 6，圖 3（a）中裝置 1 廣播一個 Announcement 作為服務要求訊息，由於裝置 2、3 和 5 分別擁有 a1、a2 和 a3 這三種 type a 的服務，因此回傳 Bid 訊息如圖 3（b）所示，內容記載服務相關資訊如裝置能提供的頻寬、服務品質及來源等以計算信任值，讓服務要求者（裝置 1）由這些 Bid 訊息中找出最符合自己所需的服務，或是如圖 3（c）由於裝置 6 和裝置 5 互動過，所以可以回傳名聲參數作為建議讓裝置 1 參考，最後在圖 3（d）中裝置 1 根據收到的 Bid 選擇給予裝置 5 Award 訊息，以此方法完成服務探尋的動作。由於本文使用的服務探尋方法是以點對點及轉傳的方式進行資訊的交換，並用 SCM 儲存服務提供者之服務資訊，所以在圖 3（d）可以看到裝置 1 會將所得到的服務資訊[a1, #5]、[a2, #2]、[a3, #3]以及名聲[#5,a1,**]儲存於 SCM 中，如同裝置 4 因為轉傳的方式同樣的會將服務資訊[a1, #5]及[#5,a1,**]暫存於 SCM，以保留於將來需要相同服務時使用，如此可節省重複要求相同服務時所耗費的資源，加快尋找服務的速度，有助於提升服

務探尋的效率。

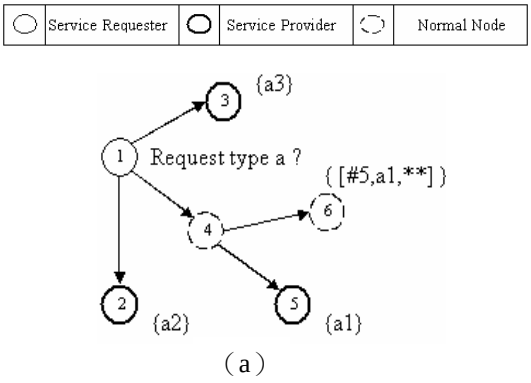


圖 3、Service Request Procedure using CNP
（a）Query （b）Bid Return
（c）Reputation Return （d）Award

### 3.2 第二階段-服務選擇評估

上一節以 CNP 作為代理人溝通協商進行服務探尋，找出環境中存在需要的服務，或是得到與所需服務相關的資訊，並將進行服務的選擇和判斷。由於在 MANET 環境中每部連網裝置所提供的服務可能會有重複的情形，且不排除裝置為惡意裝置之可能性，所以在選擇最有效益的服務和判斷惡意行為部分就顯得重要，因此為了使服務探尋具效率、安全及穩定性，本研究延續第一節所探討的服務探尋架構，加入了代理人誠信機制，利用 FCM 的方法對服務提供者進行能力評估，以及參考名聲及經驗（Experience）參數來選擇最佳的服務提供者達到學習與選擇，並防止惡意裝置企圖以惡意行為癱瘓本研究所建立的誠信機制。

圖 4 為本研究所使用的 FCM 樹狀圖，用以作為服務的判斷決策。此信任值計算機制不僅可以對環境所發生的情況比重不同做出調整權重的應對方法，找出最符合使用者預期的服務，還能對於服務效率較差的裝置，利用 FCM 降低其信任值，只在無其他服務提供者的情況下才會去使用信任值較低之服務；對於有惡意使用者想要進行破壞行為，其名聲值也會因惡意的行為而快速下降，如此一來就能減低惡意使用者對環境造成的影響。

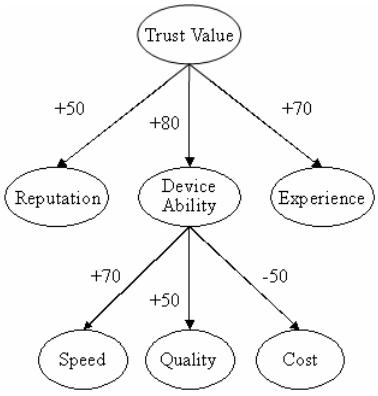


圖 4、Trust Value Computation FCM

這裡以五種會造成服務探尋效率受影響的情況作說明，分別是效率不如預期（Unexpected）、偽裝（Naive）、偽善（Hypocritical）、謊報（Pseudo Spoofing）及聯合欺騙（Collaborative）[3]，本文以 3.1 節中所提到的 SCM，來降低上述五種情況對服務探尋機制的影響，五項分別說明如下：

情境 1. 效率不如預期

當發生服務提供者的服務效率與當初所簽訂的合約不同，造成效率不如預期的情況，則代理人會將真實的情況紀錄下來，包括服務的速度、成本和品質，並使用 FCM 再作一次評估，得到一個新的、較低的信任值，然後存放於 SCM 中作為如『過往經驗』紀錄，當成扣分的依據。所以在服務的效率低落或服務中斷時，代理人就會給予違約的扣分，並由之前暫存的 Bid 訊息中尋找替代方案，要求新的服務來繼續完成工作。圖 5 所示即為以 SCM

紀錄信任值的變化，解決當效率不佳情況發生時代理人的應變方法。圖 5（a）為經過 FCM 以表 1 所計算得到的每個服務提供者信任值（Computed Trust Value），由於裝置 1（ID-1）所被評估出來的信任值為最高 94，根據本文所提出的方法則會挑選此服務提供者；不過當經過互動後發現有效率不如預期的情形，則根據互動時的狀況以 FCM 計算新的信任值（Assessment Trust Value），如圖 5（b）中實際的速度、品質和成本分別降低為 40、40 和 60，所以得到新的信任值為 63，將此新值紀錄在 SCM 中以供之後當作經驗參數或提供給其他裝置當名聲用。

表 1、Service Ability Parameter

| Service | Provider | Speed | Quality | Cost | Trust Value |
|---|---|---|---|---|---|
| A1 | ID-1 | 100 | 100 | 20 | 94 |
| A2 | ID-2 | 85 | 60 | 40 | 88 |
| A1 | ID-3 | 70 | 60 | 45 | 85 |
| A3 | ID-4 | 60 | 60 | 60 | 74 |

| Service | Provider | Computed Trust Value |
|---|---|---|
| **A1** | **ID - 1** | **94** |
| A1 | ID - 3 | 88 |
| A2 | ID - 2 | 85 |
| A3 | ID - 4 | 77 |

（a）

| Service | Provider | Computed Trust Value | Accessed Trust Value | TTL |
|---|---|---|---|---|
| **A1** | **ID - 1** | **94** | **63** | **1030** |
| A2 | ID - 3 | 88 | -- | 1000 |
| A1 | ID - 2 | 85 | -- | 1000 |
| A3 | ID - 4 | 77 | -- | 1000 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

（b）

圖 5、SCM with Unexpected Situation
（a）Compute Trust Value before Interaction
（b）Store the Trust Value after Interaction in SCM

情境 2. 偽裝

當代理人發現服務提供者為惡意裝置、取得的服務或下載的檔案是由惡意軟體所偽裝，處理的方式可以視為效率不佳的情況，只是所扣的分數可以加重，防止自己再去使用有問題的服務，並提供自己的經驗給其他需要相同服務的代理人作為『名聲值』，以類似警告的方式告知別的要求者。圖 6 即是以 SCM 表達發生偽裝情形時的解決方式，若是發現服務提供者為惡意裝置，例如圖中的裝置 1 為提供惡意軟體的裝置，則給予極低的評價（最低可為 0）來計算新的信任值（Accessed Trust Value, 圖中以**表示），以極低的信任值讓要求端之後不再信任此提供者，降低之後與之來往的機會，間接減少服務探尋失敗的次數。代理人也會將此信任值當成名聲提供給其他裝置作為警告，讓別的服務要求代理人降低對此惡意裝置的信任值，使得此惡意服務提供者所提供的惡意軟體漸漸不被挑選及下載，有效提升服務探尋成功率。

情境 3. 偽善

當惡意裝置提供惡意程式，且為了規避上述信任機制而進行偽善的惡意行為，讓代理人無法使用實際有效的經驗參數，所以本研究使用紀錄歷史經驗的方法（如公式 3-1，方法於稍後描述），其計算概念為參考之前的互動經驗，暫存代理人間服務的互動過程，降低偽善情況所造成的影響。此一情形 SCM 的表達方式與圖 5 類似，依然將新的信任值儲存於 SCM 的 Accessed Trust Value 中以供之後參考，或提供給其他裝置作為名聲參數之用。

| Service | Provider | Computed Trust Value | Accessed Trust Value | TTL |
|---|---|---|---|---|
| **A1** | **ID - 1** | **94** | ** | **1030** |
| A2 | ID - 3 | 88 | -- | 1000 |
| A1 | ID - 2 | 85 | -- | 1000 |
| A3 | ID - 4 | 77 | -- | 1000 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

圖 6、Differ the Malicious Action using SCM

情境 4. 謊報

若發生有惡意裝置謊報自己的裝置能力，欺騙服務要求者使用自己所提供有惡意的軟體，對此情形最直觀的解決方式是將名聲參數的比重在 FCM 中調低，減少謊報情況的影響，不過如此一來名聲參數就沒有意義，違背原本 FCM 的設計要素。若是以 SCM 所暫存的資料來降低謊報情形的影響，可以依效率不如預期或提供惡意軟體之方式（如圖 3. 9 或圖 3. 10）來計算真實的信任值，如此再遇到同一個謊報的裝置時，使用其所提供的惡意服務機會將會變的極低。

情境 5. 聯合欺騙

當環境中出現聯合謊報名聲的裝置，企圖以不正確的信任值計算癱瘓代理人誠信機制，則必須要有一個辦法能讓代理人發現名聲值是不可信的。本研究所使用的方法是以類似『加權（Weighted）』的方式，若出現實際互動後的結果和推薦的名聲值差距太大，甚至發現是惡意軟體，則必須要注意使否為惡意裝置進行謊報行為，開始對其所提供的名聲

值產生懷疑，改變此名聲值對整體信任參數計算的影響（名聲值權重計算將稍於後公式 3-2 說明）。如圖 7（a）中評估裝置 1 的信任值因為效率不佳或提供病毒，而由 94 變為實際的 20，比照圖（b）中 SCM 暫存的名聲值資料，發現裝置 7 給予裝置 1 的名聲評價為 90，與實際互動的經驗差距大於一個門檻值，代表裝置 7 可能有謊報他人名聲的惡意行為，因此降低推薦人（裝置 7）所提供的名聲參數對信任值計算之影響，若真確為聯合欺騙的行為，則能在幾次學習後不再相信此推薦人所提供之名聲值。

| Service | Provider | Computed Trust Value | Accessed Trust Value | TTL |
|---|---|---|---|---|
| A1 | ID - 1 | 94 | 20 | 1030 |
| A2 | ID - 3 | 88 | -- | 1000 |
| A1 | ID - 2 | 85 | -- | 1000 |
| A3 | ID - 4 | 77 | -- | 1000 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

（a）

| Service | Provider | Reputation | Recommend Device | TTL |
|---|---|---|---|---|
| A2 | ID - 3 | 80 | ID - 6 | 1210 |
| A1 | ID - 1 | 90 | ID - 7 | 1210 |
| A1 | ID - 2 | 86 | ID - 5 | 1210 |
| A3 | ID - 4 | 77 | ID - 8 | 1210 |
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |

（b）

圖 7、Weighted Reputation using SCM
（a）The Experience after Interact
（b）Check the Reputation Table and find Malicious Device

綜合上述解決方法，本研究使用 FCM 和 SCM，讓代理人能學習判斷惡意行為，在破壞尚未影響整個的計算如式 1 ，其中 $exp_i$ 為互動紀錄中第 i 次的經驗，也就是第 i 次互動時的信任值， $n$ 為互動 n 次所紀錄的互動經驗，利用這 n 次互動的經驗計算，所得到的平均值就是根據歷史紀錄而得到的經驗參數 $EXP_k$，即為某部裝置對裝置 k 所紀錄的過往經驗參數。當發生惡意裝置將惡意軟體或檔案偽裝成正常服務時，則經過互動後服務要求代理人對其信任值會快速降低，往後互動機會就變小，甚至偏向於不再互動；而在出現惡意裝置以偽善的方式進行欺騙時，雖然其一開始會讓代理人產生誤判，但因為經驗參數能綜合歷史紀錄，所以其信任值也會逐漸降低，減少往後互動的機會。

$$EXP_k = \frac{1}{n}\sum_{i=1}^{n}(exp_i) \quad (1)$$

k : Device k
$EXP_k$ : Interaction experience with device k
$exp_i$ : The i'th interact experience with device k
n : Total interact times with device k

至於名聲值的計算方法論述如下，$REP_k$ 為服務提供者 k 的名聲，$EXP_{j\_k}$ 則是以與 k 互動過的其他裝置 j 的信任參數，$\Psi_j$ 為對裝置 j 所提供之名聲的可信度，參數 Ψ 為控制提供名聲值結點的影響力，Ψ 參數數值如式 2，是介於 0 到 1 之間的數，對於一般正常的裝置其 Ψ 值為 1，而當獲得的名聲和實際互動情況差異太大，則代表有可能出現謊報的情況，因此累加常數 $c$ 值，每次減掉 0.2 的影響權重，直到 $c$ 大於等於 4 時（Ψ 小於 0.4），則不再考慮此點所提供的名聲值參數，也就是將其列入黑名單中。得到 Ψ 值後即可計算出符合實際情況的名聲值 $REP_k$，如公式 3 所示 $REP_k$ 之值可由 $EXP_{j\_k}$ 乘以 $\Psi_j$ 再除以 N 個提供名聲的裝置而得到。

$$\Psi = \begin{cases} 1\ , \text{ the first time interact with the node or a normal node} \\ 1-(0.2*c)\ , \text{ if } 0<c<3\ , c\in Z \\ 0\ , \text{ if } c\geq 4\ , c\in Z \end{cases} \quad (2)$$

$c$ : The number of lies recorded

$$REP_k = \frac{1}{N}\sum_{j=1}^{N}\Psi_j * EXP_{j\_k} \quad (3)$$

$REP_k$ : Reputation about device k
$EXP_{i\_k}$ : Device j's experience about device k
$N$ : Total reputation from other devices
$\Psi_j$ : Effect of device j

## 4. 模擬分析

本研究實驗程式使用 Borland C++ Builder 6.0 平台開發，模擬在 MANET 環境下進行服務探尋和選擇，並加入 FCM 演算法作為代理人判斷決策的核心方法。本文架構著重於利用代理人誠信機制作準確的服務探尋，有效的提升服務成功率（Service Availability）。服務成功率的定義如式 4，為成功的服務探尋次數除以總共發出的要求動作次數，在最好的情況下服務探尋機制服務有效度為 1，也就是發出要求訊息後都能得到網路內所需要的服務。本實驗假設模擬的網路環境內擁有 N 部裝置，這 N 部裝置將隨機加到模擬環境內，根據其加入順序給予 ID-1 到 ID-N 的編號，其中有 P%的機會裝置將會扮演服務提供者，因此環境中會有 NP 個服務提供者的存在，每個服務提供者由 10 個預設的服務陣列

{a1, a2, a3, s1, s2, w1, w2, w3, q1, q2}中隨機給予 2 個服務。模擬流程第一步為設定模擬環境，給予裝置數目、能力及惡意裝置，第二步驟則在加入環境的同時會發送廣告訊息給鄰近的裝置，然後服務提供者就等待要求者發送要求訊息，接下來第三步開始模擬服務要求動作，比較以 FCM 作為代理人判斷決策方式和以隨機挑選方式選擇服務，觀察服務探尋成功率的變化情形，用第四步驟的代理人溝通協商 CNP 及 FCM 服務選擇評估來模擬本文所提出的服務探尋與選擇架構。

$$\text{Service Availability(SA)} = \frac{\text{Succeeded Query Times}}{\text{Total Query Times}} \quad (4)$$

為了模擬效率不如預期情形，程式中設定每個服務提供者皆有其能力等級，隨機分成『優』、『佳』、『普通』、『不佳』和『劣』五種，代表裝置的速度、品質及成本所能分配到的能力範圍（0 到 100），而這五種等級的服務提供者將分別有 10%、30%、50%、70%和 90%的機會無法正常提供服務，也就是會造成服務失敗或效率不如預期的狀況，使得服務成功率降低，如此即可觀察服務成功率的變化情形。圖 8 為 N 等於 30 和 NP 等於 10 的環境變數下效率不如預期情況以 FCM 和隨機挑選方式的服務成功率比較，由於以 FCM 為選擇機制的方法所挑選的服務提供者通常是能力較高的裝置，其服務失敗率普遍較低，所以其服務成功率都能比以隨機挑選的方式好。

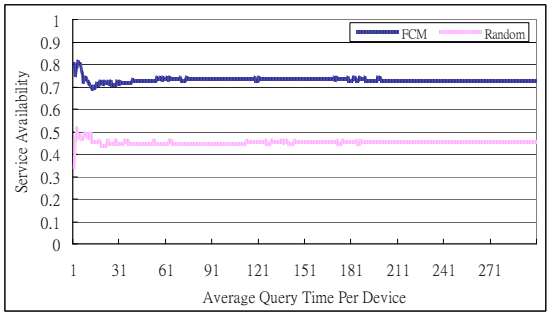


圖 8、Service Availability with Unexpected Situation

如圖 9 所示，實驗設定惡意裝置占服務提供者的 50%，平均每部裝置進行 300 次的服務要求時，雖然一開始整體的服務成功率下降，但是以 FCM 的判斷選擇方式，依然能比隨機選擇服務的方式之服務成功率佳，並且因為經驗和名聲參數，大約在平均每部裝置進行 4 次的服務要求後，以 FCM 的方式能夠使服務成功率慢慢上升，也就是因為服務要求者漸漸的不與有惡意行為的裝置進行互動，有效的降低惡意裝置對環境的破壞。

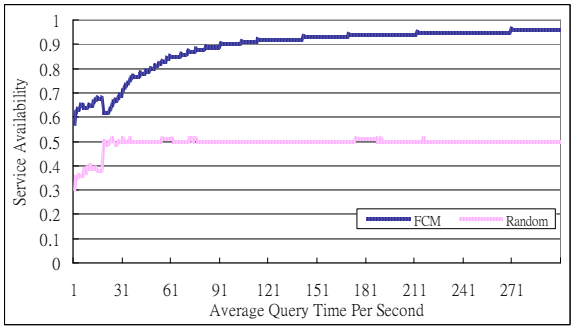


圖 9、Service Availability with Naive Situation

為了模擬偽善情況，程式設定所有的惡意裝置在一開始並不會提供惡意軟體，在平均每個服務提供者前 3 次的服務要求皆提供者正常服務，但在 3 次的服務要求之後，惡意裝置會將正常服務改成偽裝的惡意軟體，讓服務要求者因受到欺騙而下載到惡意軟體。圖 10 為環境中存在有服務提供者 50%的惡意裝置服務探尋及選擇的服務成功率變化情形，在前 3 次的平均服務要求中，探尋成功率皆為 1，但之後進行的服務要求，由於惡意裝置開始偽裝惡意軟體，所以服務成功率會開始下降，以隨機挑選服務的方式其服務成功率最後會在 0.5 左右，而以 FCM 來判斷決策，其服務成功率雖然在一開始時會降低，但大約在平均每部裝置進行 20 次要求動作後會慢慢提升，最後服務成功率能落在 0.9 以上，代表在占服務提供者 50%的惡意裝置中，以平均歷史經驗的計算方式的確能讓服務探尋的成功率比隨機挑選的方式好，防止惡意裝置以偽裝行為對服務探尋機制造成影響。

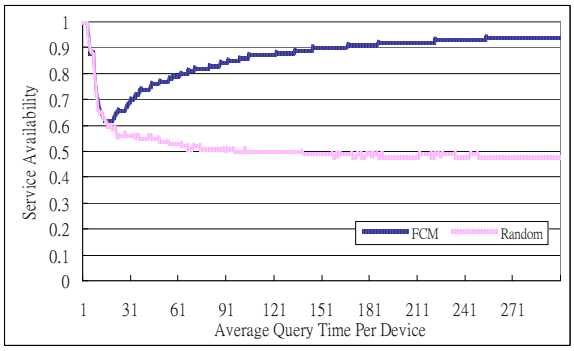


圖 10、Service Availability with Hypocritical

本實驗設計環境中的惡意裝置謊報其速度為 90、品質為 90 及價格為 30，預設經驗為 75、名聲為 80，以 FCM 計算所得到的信任值為 83，這在本實驗中所預設的裝置能力相較下是非常高的，因此會讓沒與之互動過的服務要求者因受騙而選擇有惡意的服務提供者；而因為本實驗的服務要求者與服務提供者互動後，會確認服務時所得到真正服務效率（速度、品質和價格等），因此能得到實際的信任值，並將此次的互動經驗暫存及提供給他人作

為名聲，儘量避免其他裝置受到惡意服務提供者的欺騙，提高服務探尋的成功率。圖 11 為當環境中有占服務提供者 50%的惡意裝置存在，比較有無使用 FCM 方法的服務成功率，由圖中可以看出因為以隨機挑選的方式沒有經過裝置能力、經驗或名聲的判斷，所以其服務成功率約在 0.5 左右，而以 FCM 選擇的方法會因為供判斷的參數錯誤，導致一開始服務成功率低落，但可以看出在第 20 次後的平均服務要求後，其成功率將會因為判斷和紀錄，排除不可信任的服務提供者，而慢慢提升服務成功率。

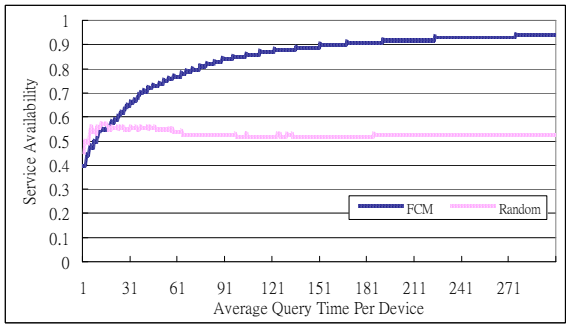


圖 11、Service Availability with Pseudo Spoofing

當環境中的惡意裝置除了謊報自己的能力，甚至還以聯合的作法給予別的惡意裝置極高的名聲及給予正常裝置不好的名聲，如此一來會讓 FCM 獲取錯誤的名聲，得到不正確的信任值，導致每次所挑選出來的服務經常是惡意裝置所提供，所以服務探尋的成功率將會變低。在聯合欺騙的模擬中，實驗設計惡意裝置不僅會竄改自己的能力值，這裡還設定所有惡意裝置都是同一個欺騙的群組，每部惡意裝置都會在服務要求者發出服務要求訊息時提供假的名聲，謊報其他惡意裝置之名聲為 90，以及將正常善意的裝置之名聲謊報為 10，因此會得到如圖 12 結果，可以看到在平均服務要求次數第 24 次之前，以 FCM 為判斷決策方式因為受到欺騙，所得到的信任值是不正確的，因此其服務成功率非常的低，但之後因為服務要求者經過互動後慢慢的發現並忽略錯誤的資訊，將謊報的裝置提供的資訊之可靠度 Ψ 降低，所以在平均第 24 次之後的服務要求成功率能夠比以隨機挑選方式還好。

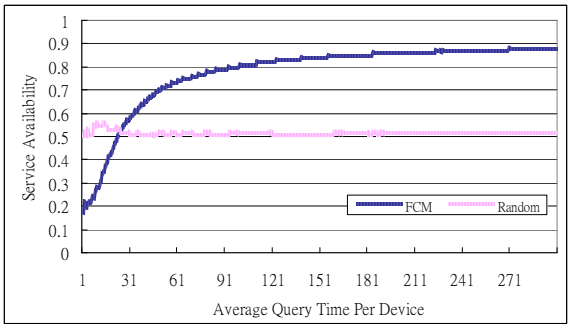


圖 12、Service Availability with Collaborative

以上實驗討論在相同裝置數（30）、相同服務提供者數（10）和占服務提供者數 50%惡意裝置的環境條件下，對於五種惡意行為其服務探尋成功率的差別，圖 13 則為以上實驗之整理列表，並以變動模擬環境中的裝置數及惡意裝置數（占服務提供者 20%、50%和 80%數量的惡意裝置），提升為 50 部裝置、20 部服務提供者和進行 1000 服務要求，以及 100 部裝置、50 部服務提供者和進行 2000 次服務要求，讓每部裝置平均都能進行 20 次的要求動作，並模擬 100 次取平均值，來觀察本研究避免惡意行為的方法在裝置數較多的環境中所能提升之服務成功率。提升之服務成功率計算，是以本研究以 FCM 方法之服務成功率減去以亂數方法之服務成功率，再除以亂數方法之服務成功率百分比。所得到的提升率即為圖 13 所示，由表中可以看到效率不如預期情況下所提升之服務成功率最大，而各種惡意情境（偽裝、偽善、謊報及聯合欺騙）下則有機會能在越多惡意裝置或惡意行為出現時得到更高的服務成功率，如在情境 2 偽裝方案中，80%惡意裝置情況下其提升之服務成功率大於 50%和 20%惡意裝置情況，證明本研究所使用的 FCM 及經驗、名聲計算系統之有效性。

| **30 Devices, 10 Providers** | | | | | |
|---|---|---|---|---|---|
| Malicious Device | Scenario 1 | Scenario 2 | Scenario 3 | Scenario 4 | Scenario 5 |
| 20% | 42% | 16% | 12% | 6% | 17% |
| 50% | | 26% | 17% | 19% | 16% |
| 80% | | 37% | 16% | 28% | 25% |
| **50 Devices, 20 Providers** | | | | | |
| Malicious Device | Scenario 1 | Scenario 2 | Scenario 3 | Scenario 4 | Scenario 5 |
| 20% | 50% | 14% | 10% | 11% | 14% |
| 50% | | 25% | 13% | 28% | 26% |
| 80% | | 36% | 15% | 43% | 39% |
| **100 Devices, 50 Providers** | | | | | |
| Malicious Device | Scenario 1 | Scenario 2 | Scenario 3 | Scenario 4 | Scenario 5 |
| 20% | 54% | 10% | 8% | 13% | 10% |
| 50% | | 20% | 10% | 34% | 20% |
| 80% | | 34% | 10% | 40% | 23% |

圖 13、Average Simulation Result

## 5. 結論

鑒於行動裝置數量的提升及 MANET 環境的運用，本文提出一個完整的服務探尋及選擇架構，使用代理人技術來幫助使用者在 MANET 環境下進行服務探尋，設計 ECNP 作為代理人溝通協商方式達到服務要求的動作，以搜尋使用者所需要的服務；並加入誠信機制讓代理人能夠在多個相同服務中選出最合適的，利用 FCM 的方法對提供服務的裝置作一個優劣的評定，根據與服務提供者的互動情況及名聲作即時性的調整，找出可以信任的裝置及阻斷惡意裝置的干擾。

本文將服務探尋機制分成兩個部分，第一部分是服務的尋找，利用 CNP 作為代理人互動、分享資

訊的協定，並加強 CNP 成為 ECNP 讓代理人溝通協商能更適用於 MANET 環境，包括工作的同時進行和動態解除合約，以提升服務探尋機制的效率；第二部分則使用 FCM 演算法作為代理人誠信機制，以速度、品質和成本來評定某個服務提供者的能力，及根據此服務提供者的名聲和互動的過往經驗，讓服務要求代理人判斷選擇最適合、最可信任的服務，及早遏止惡意裝置對整個網路環境造成影響，提高服務探尋機制的正確性及安全性。實驗結果中可以看到本研究所提出的架構能提升服務探尋機制的成功率，除了能選擇最適合使用者所需的服務，還能有效降低某些惡意行為對誠信機制所造成的影響，提升服務探尋的效率。

## 參考文獻


[1] R. M. Axelrod, "Structure of Decision: the Cognitive Maps of Political Elites," Princeton University Press, Princeton, New Jersey, 1976.

[2] A.S. Ali, S.A. Ludwig, O.F. Rana "A cognitive trust-based approach for Web service discovery and selection," Third IEEE European Conference on Web Services, Nov. 2005.

[3] F. Aydin, E. Uzun and Mark R. Pariente, "A reputation-based trust management system for P2P networks," IEEE International Symposium on Cluster Computing and the Grid, pp. 251-258, Apr. 2004.

[4] J.R.D. Dyson, N.E. Griffiths, C. K. Lim, S.A. Jarvis, G.R. Nudd "Trusting agents for grid computing", IEEE International Conference on Systems Man and Cybernetics, Vol. 4, pp. 3187-3192, Oct. 2004.

[5] F. K. Hussain, E. Chang and T. Dillon "Defining Reputation in Service Oriented Environment," International Conference on Internet and Web Applications and Services, Feb. 2006.

[6] S. Helal, N. Desai, V. Verma and C. Lee, "Konark-A Service Discovery and delivery protocol for ad hoc networks," Proceedings of IEEE Wireless Communications Networking Conference, Vol. 3, pp. 2103-2113, March 2003.

[7] B. Kosko, "Fuzzy cognitive maps," International Journal of Man-Machine Studies, Vol. 24, No. 1, pp. 65-75, 1986.

[8] U.C. Kozat and L. Tassiulas, "Service Discovery in Mobile Ad Hoc Networks: an Overall Perspective on Architectural Choices and Network Layer Support Issues," Elsevier Science, Ad Hoc Networks, Vol. 2, no. 1, Jan. 2004.

[9] U.C. Kozat and L. Tassiulas, "Network Layer Support for Service Discovery in Mobile Ad Hoc Networks," In Proceedings of IEEE Computer and Communications Societies, Vol. 4, No. 4, pp. 1965-1975, Apr. 2003.

[10] C. Lee and S. Hela, "Protocols for Service Discovery in Dynamic and Mobile Networks," International Journal of Computer Research, Vol. 11, N0. 1, pp. 1-12, 2002.

[11] C. Lee, A. Helal, N. Desai, V. Verma, and B. Arslan , "Konark: A System and Protocols for Device Independent, Peer-to-Peer Discovery and Delivery of Mobile Services," IEEE Transactions on System, Man, and Cybernetics, Vol. 33, No. 6, pp. 682-696, Nov. 2003.

[12] X. Li and L. Ling "PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities," IEEE Transactions on Knowledge and Data Engineering, Vol169, No.7, pp. 843-857, July 2004.

[13] Y. Miao and Z.-Q. Liu,"On causal inference in fuzzy cognitive maps," IEEE Transactions on Fuzzy Systems, Vol. 8, No. 1, pp. 107-119, Feb. 2000.

[14] B.A. Miler, T. Nixon, C. Tai and D. Wood, "Home Networking with Universal Plug and Play," IEEE Communications Magazine, Vol. 39, No. 12, pp.104-109, Dec. 2001.

[15] M. Nidd, "Service Discovery in DEAPspace," IEEE Personal Communication, Vol. 8, No. 4, pp. 39-45, Aug. 2001.

[16] E.I. Papageorgiou, C.D. Stylios and P.P. Groumpos, "An integrated two-level hierarchical system for decision making in radiation therapy based on fuzzy cognitive maps," IEEE Transactions on Biomedical Engineering, Vol. 50, No. 12,pp. 1326-1339, Dec. 2003.

[17] G. G. Richard, "Service Advertisement and Discovery: Enabling Universal Device Cooperation," IEEE Internet Computing, Vol. 4, No. 5, pp. 18-26, Oct. 2000.

[18] Reid G. Smith, "The Contract Net Protocol: High-Level Communication and Control in a Distributed Problem Solver**,"** IEEE Transactions on Computers, Vol. C-29, No. 12, pp. 1104-1113, Dec. 1980.

[19] S. Song, K. Hwang, R. Zhou and Y.-K. Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation," IEEE Internet Computing, Vol.9, No.6, pp. 24-34, Dec. 2005.

[20] Y. Wang and J. Vassileva "Bayesian network-based trust model",Proceedings IEEE/WIC International Conference on Web Intelligence, pp. 13-17, Oct. 2003.

[21] F. Zhu, Matt W. Mutka and Lionel M. Ni, "Service discovery in pervasive computing environments," IEEE Pervasive Computing, Vol. 4, No. 4, pp. 81-190, Dec. 2005.

[22] Bluetooth, Specification of the Bluetooth System, Specification vol. 2, http://www.bluetooth.com

[23] Fuzzy Cognitive Maps Web Side, http://www.ochoadeaspuru.com/fuzcogmap