採用蟻行最佳化演算法分析網路路由及追蹤阻斷服務攻擊來源

邱泰毓
義守大學資訊管理學系
caster5210@yahoo.com.tw

劉振隆
義守大學資訊管理學系
jlliu@isu.edu.tw

摘要

本文提出一種由螞蟻覓食行為啟發出來之蟻行演算法以路徑上費洛蒙濃度吸引螞蟻群以搜尋出最佳路徑，並應用於網路路由、驛馬車以及阻斷攻擊追蹤等問題。演算法包含各項參數之使用，如費洛蒙濃度參數、距離(網路流量)參數、區域更新參數。由於完成一個大型網路路由計算的資源消耗大，搜尋最佳路徑前將篩選多條路徑來進行分析。實驗中將分析 9、14、52 個節點數的網路路由，10 個節點的驛馬車問題、20 至 40 個節點不等以及缺乏完整性網路流量的阻斷攻擊追蹤分析，期能得到最佳路徑之搜尋結果。

關鍵詞：蟻行演算法、阻斷攻擊、網路路由計算。

Abstract

This study uses an Ant Colony Optimization (ACO), which inspired by the foraging behavior of real ants and distributed the pheromones on the path in order to attract ants to pass through the path, and applies to the simulations of network routing, stagecoach and Denial of Service (Dos) traceback problems. There are some parameters include pheromone, distance (or octet), and local updating rule. If we want to conduct a large size network router computing, the computation will become complexity and also consume a large number of resources. Therefore, it will be a good choice to analyze some tours before searching the optimal tour. This study will analyze network router networks with 9, 14, 10 and 52 nodes, DOS traceback problems with 20 to 40, and some cases without octet nodes for the purpose of obtaining optimal searching tours.

Keywords: Ant Colony Optimization (ACS), Denial of Service (DOS), Network Router Computing.

1. 簡介

近年來網路的進步，給予企業與個人帶來相當的便利。但也正因如此，導致了一些難以解決的致命危機，由於作業系統隱含不可避免的漏洞以及相關防護措施的不齊全，使得駭客有機可圖，利用各種方法如特洛伊木馬病毒(Trojan)、蠕蟲(Worm)以及阻斷攻擊(Denial of Service 等，於各大企業資料庫中入侵竊取資料或使其運作異常，甚至將其破壞、癱瘓。根據 Crime-Research 網站[14]每年統計的損失均超過幾十億甚至達百億美元，數量相當可觀，且阻斷服務攻擊於每年均為大型電腦的經濟犯罪之一。如美國各大型網站 Amazon、Yahoo、Ebay 等，也都曾遭受到阻斷攻擊。阻斷攻擊的特性為利用大量的封包傳送至目的地，由於網路伺服器及路由器具有一定的頻寬及硬體上的限制，若傳送的封包數量超出處理的上限，則當達到完成阻斷攻擊的任務時，會影響網路服務的品質，甚而完全癱瘓。

為了解決此項問題，本文提出一種以蟻行演算法的追溯(Traceback)方法，找出攻擊的來源。本篇論文將以 TSPLIB 題庫 [19]做為網路路由器(Network Routing)路徑範例、驛馬車問題(Stagecoach Problem)以及 Dos 攻擊來源回溯等問題進行分析結果與相關驗證，並利用 NS-2(Network Simulator 2) [25]模擬網路環境架構。

蟻行演算法由 Dorigo et al. [16, 17]所提出的一種啟發式演算法(Heuristic Method)，以自然界的螞蟻做為模擬的對象，用以搜尋最短路徑問題上。當螞蟻在尋找食物時，會在地上留下一種分泌物稱為費洛蒙拖曳物(Pheromone Trail)，使得蟻群對於要走的路線將有成正比例的效果。假設越來越多的螞蟻走過相同的路徑時，路徑上的費洛蒙濃度將逐步增加，因此堆積費洛蒙越多的路徑上將會吸引更多的螞蟻選擇該條路徑，如圖 1 所示，可說明螞蟻群搜尋最短路徑之過程。

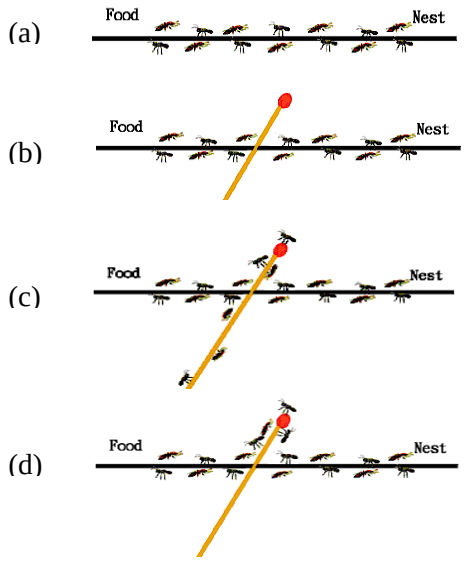


圖 1 螞蟻由蟻巢為起點搜尋食物之路徑示意圖，圖(a)無設置障礙物之路徑，圖(b)設置一火柴為障礙物，圖(c)搜尋最佳路徑，圖(d)最佳路徑搜尋完成圖

在圖 1(a)中，螞蟻由右端蟻巢出發前往左方覓食，一開始螞蟻循直線前進。圖 1(b)顯示通往食物的路徑上擺設了障礙物(Obstacle)，而導致岔路的情況，形成了岔路兩條距離不等的路徑。一開始，行走這兩條路徑的機率相同，但因上方的路線(為較短路徑)之螞蟻可較快速越過障礙物而到達食物的地點。圖 1(c)顯示出由於障礙物的阻擋致使路徑的長短不一，所以選擇上方路線行走的螞蟻越過障礙物取得食物並往回走到分岔路的數量較多，也同時留有較多的費洛蒙量。反之，因往下方行走的螞蟻數量較少，所累積的費洛蒙量也相對較少。在正向回饋(Positive Freeback)模式影響下，經過幾次疊代後，大多數的螞蟻將趨向於選擇往上方路線之最短路徑行走，(如圖 1(d))。

2.研究方法

2.1 螞蟻演算法之流程與結構

Psedo-code: ACO algorithm

```
Begin
    for 1 to n do
        Ant generation();
        Ant activity();
        Pheromone compute();
        Best Path memory();
    End;
End;
```

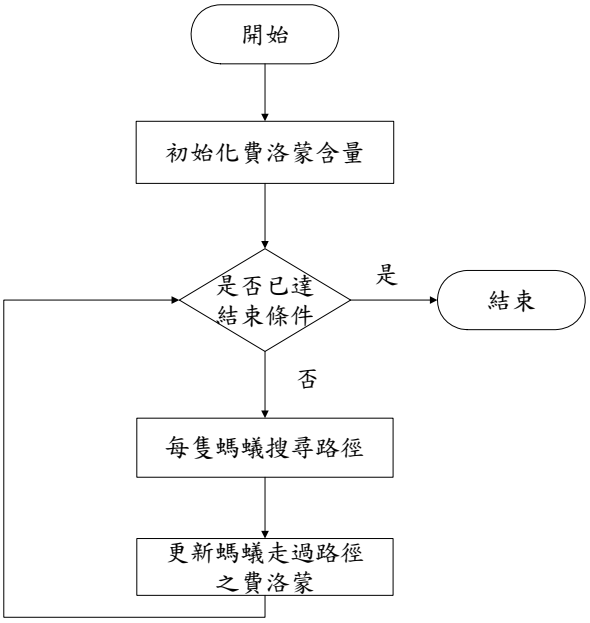


圖 2 螞蟻演算法整體流程圖

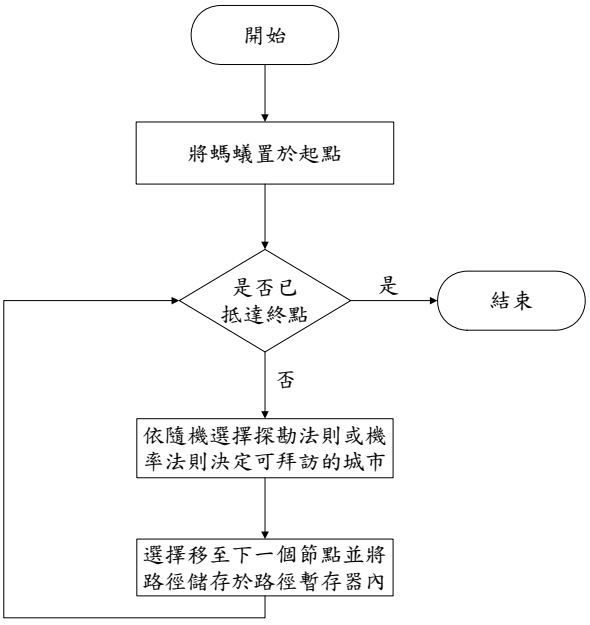


圖 3 螞蟻演算法中單一螞蟻演算流程圖

如圖 2 與圖 3 所示，螞蟻演算法求解最佳化問題的過程中，整個演算法之結束條件(Stopping Criteria)與限制條件如下:

(1)固定的疊代次數，無論搜尋結果如何，若執行到固定的回合數後將停止運算。

(2)限制不再回到已拜訪過的節點。

(3)若螞蟻已處於「邊緣點」，則表示目前已無任何相鄰的節點可拜訪，就必須強迫終止該螞蟻其拜訪工作。

其他相關影響螞蟻演算法之因素如下:

(1)整個系統中螞蟻的數量

(2)費洛蒙揮發量ρ

(3)拜訪路徑的表示方式

(4)其他作為考量選擇機率的啟發函數(如網路流量)

(5)影響選擇機率的因素間的關係比值(使用者自訂之控制參數α與β)

圖 3 螞蟻演算法中單一螞蟻演算流程圖

2.1.1 機率法則

當螞蟻開始搜尋最佳路徑時，首先以一隨機機率來決定下一節點的進行，此機率與費洛蒙強度以及網路流量相關，其中網路流量也將決定螞蟻搜尋路徑的機率。其設定機率方程式如下[16, 17]:

$$p_{ij}(t)=\frac{\left[\tau_{ij}(t)\right]^{\alpha}\cdot[f_{ij}]^{\beta}}{\sum_{u\in T_i}[\tau_{iu}(t)]^{\alpha}\cdot[f_{iu}]^{\beta}} \quad (1)$$

方程式(1)中 $p_{ij}(t)$ 為在 t 時間時做為螞蟻即將從路徑 i 拜訪下一個節點 j 的機率。$\tau_{ij}(t)$ 為 t 時間時的費洛蒙含量，f_{ij} 為總網路流量的數值，α 與 β 用以決定費洛蒙濃度及網路流量之間的相對權重值，T_i 為未拜訪過的鄰近節點集合。

2.1.2 費洛蒙更新

螞蟻會將費洛蒙遺留在走過的路徑上，此稱為費洛蒙拖曳量(Pheromone Trail)，而高濃度的費洛蒙拖曳量與低濃度費洛蒙路徑有所差異。只要有螞蟻走過的路徑，路徑上的費洛蒙濃度則會改變，也就是假設第 k 隻螞蟻從路徑 i 移至下一個路徑時，則需利用「區域更新法則(Local Update Rule)」來將路徑上的費洛蒙濃度進行更新。區域更新的主要精神說明避免出現一個強勢路徑的干擾，將大部分的螞蟻吸引至該路徑上，而導致無法有適當的搜尋新路徑的動作，來影響所得之解答精確性。各節點費洛蒙的更新方式如下[17]:

$$\tau_{ij}(t+1)=\rho\cdot\tau_{ij}(t)+\Delta\tau_{ij}(t,t+1) \quad (2)$$

其中 $\tau_{ij}(t+1)$ 為在時間 $t+1$ 時，路徑 i 到 j 的費洛蒙分佈值。$\Delta\tau_i(t,t+1)$ 為第 k 隻螞蟻於時間 t 至 $t+1$ 時在路徑 i 到 j 所留下之費洛蒙的單位長度的濃度，表示式如下。

$$\Delta\tau_{ij}(t,t+1)=\sum_{k=1}^{m}\Delta\tau_{ij}^{k}(t,t+1) \quad (3)$$

$$\Delta\tau_{ij}^{k}=\frac{Q}{L_k} \quad (4)$$

其中 L_k 為第 k 隻螞蟻所走過的路徑長，Q 為 Dos 攻擊路徑上的網路流量。ρ 為費洛蒙揮發度，其中 $0<\rho<1$。

2.2 網路路由前置處理

以 TSPLIB [19]資料庫範例做為網路路由的節點範例是一項相當大的排列組合問題，原理為一個節點可連至 n-1 條選擇路徑，當節點數高達 500 時，則需要有更強大的計算能力。網路路由如圖 4 所示。一個節點只保留三條通往其他節點的最短路徑，如節點 1 連至 2、3、4，其餘路徑如節點 5 則不儲存，再將篩選出的路徑及兩節點的距離放入螞蟻系統中做運算。這樣的前置處理將可提高的螞蟻系統運算的效率。

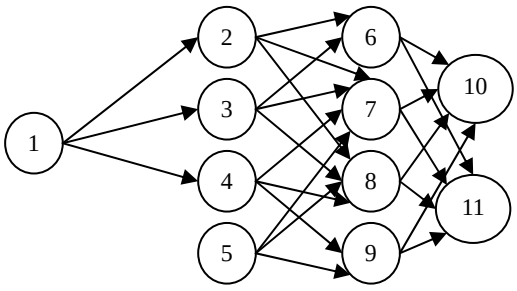


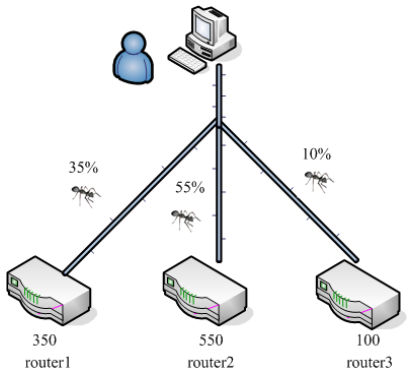
圖 4 網路路由篩選路徑圖

2.3 螞蟻系統於網路路由的應用

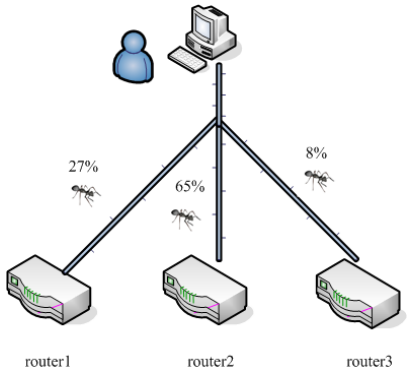
如圖 5(a)所示，遭受攻擊的電腦接受了 1000 單位的封包，分別由 router1、router2 以及 router3 所傳送 350、550 以及 100 單位，因此搜尋路徑的機率為 35%、55%以及 10%。我們將所有路徑分別放置螞蟻 35、55、10 隻，假設攻擊封包單位越大，則螞蟻所行經的數量

越多。如圖 5(b)與(c)所示，經疊代後，有更多的螞蟻群趨向於 router2，而走向其他路由的螞蟻將逐漸減少。

(a)



(b)



(c)

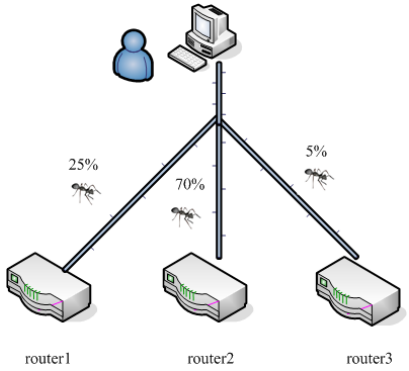


圖 5 螞蟻追蹤攻擊流量之變化情形

由於使用 IP 追溯 Dos 攻擊來源需要採用在所有攻擊路徑上使用到的路由器的流量記錄，但是，並非所有的路由器都會記錄相關的流量資訊，在此我們排除了此項缺點，在流量資訊可能會不齊全以及不添加任何經費來購置設備的情況下，利用螞蟻自動催化(autocatalytic)的特性，僅利用費洛蒙濃度來判斷 Dos 攻擊路徑。

3.實驗結果

3.1 參數組合分析

TSPLIB[19]典型範例多以各國國內各大城市座標做為範例中的實際節點，適用於搜尋最短路徑之相關問題。本文採用題庫中 Burma14、Berlin52 之節點分佈範本作為網路路由模擬路徑、驛馬車以及追蹤 Dos 攻擊路徑來源等問題之測試範例。由於搜尋最短路徑如網路路由以及驛馬車問題皆以距離做為 f_i 的設定參數，若距離越小，則該路徑被拜訪的機率越高，此與追蹤 Dos 攻擊路徑所採用網路攻擊流量越高時，則該路徑被拜訪的機率越高之特性是一致的。其它參數的設定值，如表 1 所示:

表 1 固定參數值

α	1
β	1
ρ	0.1
Q	100

3.1.1 Burma14 旅行銷售員範例驗證結果

Burma14 為 TSP 題庫中，一個模擬緬甸境內 14 個座標的範例以蟻行演算法執行 Burma14 的節點案例， 設定節點 1 為起點，節點 14 為終點。經過 10 次的重複 Runs 後，其最佳路徑長度為 11.5(整數解為 12)，最後求得之規劃路徑為 1-5-11-14，最佳路徑如圖 6 所示。

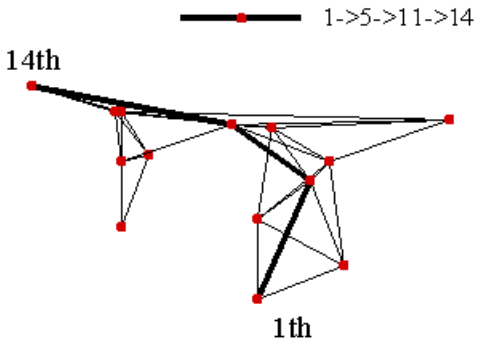


圖 6 以 ACO 執行 Burma14 之路徑結果

本案例採用 14 隻螞蟻，計算初始時將各螞蟻分別擺至 14 個節點上，則每個節點至少都有螞蟻行經，可提升解的收斂速度。經過 10 次之重複 Runs 後，其解如圖 7 所示，最後求得具有多數的螞蟻行經之最佳路徑為

1-5-11-14。

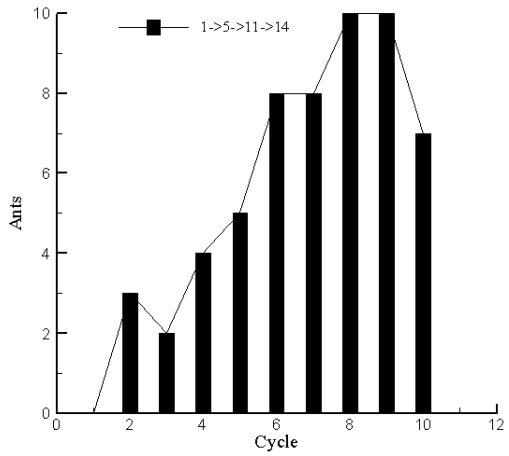


圖 7 網路路由問題之螞蟻數量結果

3.1.2 Berlin52 範例驗證結果

Berlin52 為 TSP 題庫中，一個模擬德國 52 個城市座標的典型範例，以蟻行演算法執行 Berlin52 的節點案例，設定節點 1 為起點，節點 52 為終點。經過 30 次重複 Runs 後，其最佳路徑長度為 1086.3(整數解為 1086)，途中行經 3 個節點，最後求得之規劃路徑為 1-13-28-51-52，最佳路徑如圖 8 所示。

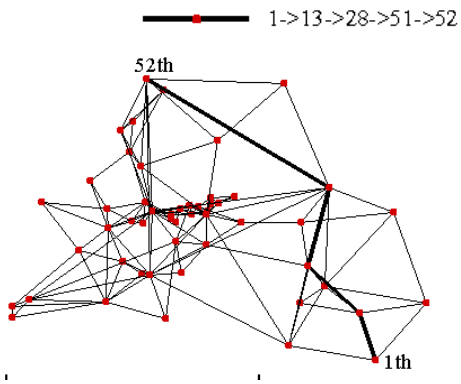


圖 8 以 ACO 執行 Berlin52 之路徑結果

如圖 8 所示，求解 Berlin52 最佳路徑問題較為複雜，經過幾次測試數量較少的 Runs 之後，發現螞蟻所搜尋之最佳路徑之螞蟻數量與路徑長度相近之螞蟻數量差異並不明顯，為了讓結果更為精確，在此系統係重複 Runs 30 次並利用 52 隻螞蟻做為設定，其解如圖 9 所示，最後求得具有多數的螞蟻行經之最佳路徑為 1-13-28-51-52。

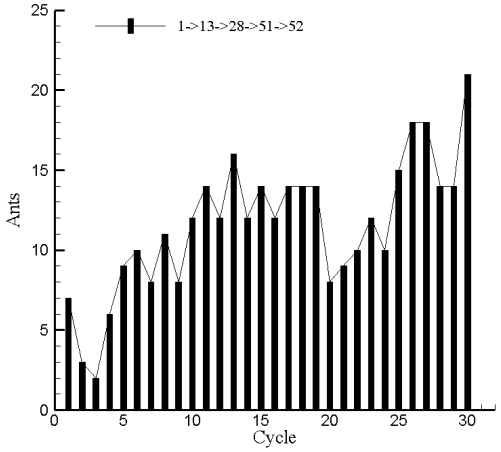


圖 9 網路路由問題之螞蟻數量結果

3.1.3 網路路由分析

網路路由案例如圖 10 所示。於此問題中，設定編號 0 為起點，編號 8 為終點。由圖 10 可知，共有三條路徑分別為 0-1-4-8、0-2-7-6-8 以及 0-3-5-4-8。而最佳路徑為 0-1-4-8，距離為 245。而解析解與文獻[10]的結果是一致的。

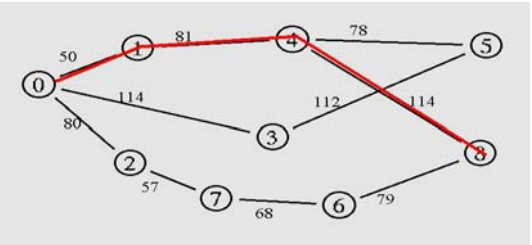


圖 10 網路路由問題搜尋最短路徑結果

此案例係重複 Runs 20 次並利用 9 隻螞蟻做為設定，其解如圖 11 所示，最後求得具有近九成的螞蟻行經之最佳路徑為 0-1-4-8。

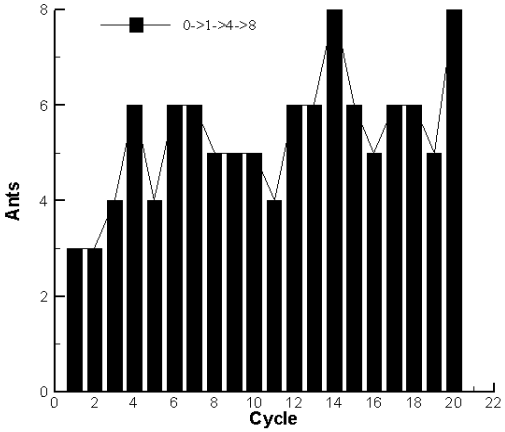


圖 11 網路路由問題之螞蟻數量結果

3.1.4 驛馬車問題分析

驛馬車問題為作業研究(Operating Research)的典型問題，於 Standford 大學 Wagner 教授提出。其原理敘述一尋寶者欲前往某地掏金，旅途中馬車將會經過危險地區，其保險費用將會增加，因此尋寶者需找出一條最安全的路徑，也是保險費最低的路徑。在此也可視為搜尋最短路徑的常見範例。圖 12 為驛馬車問題範例圖，由最左方 0 號開始為起點，直至 9 號為終點，途中包含 3 個節點，最短路徑為 0-2-5-7-9，而解析解與文獻[10]的結果是一致的。

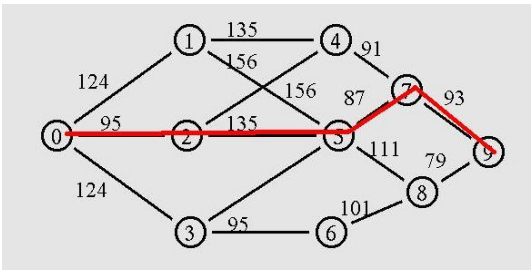


圖 12 驛馬車問題搜尋最短路徑結果

此案例係重複 Runs 15 次並利用 10 隻螞蟻做為設定，如圖 13 所示，雖然最佳路徑於疊代中途時，顯示螞蟻的數量有明顯降低的情況，而在最後幾次疊代中最佳路徑上仍陸續增加螞蟻達到約五成的數量，最後求得具有多數的螞蟻行經之最佳路徑為 0-2-5-7-9，距離為 410。

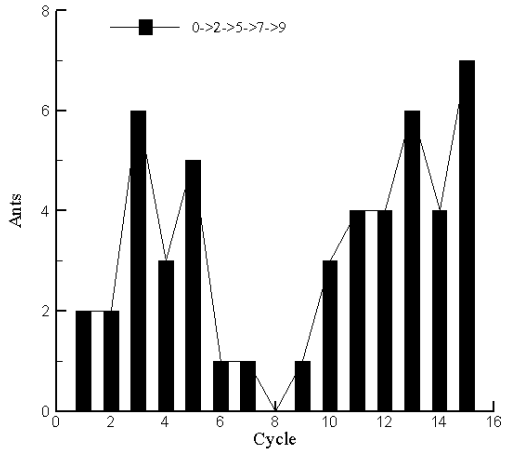
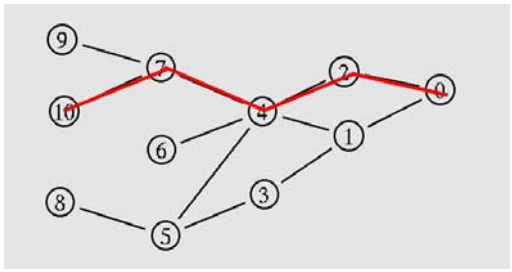


圖 13 驛馬車問題之螞蟻數量結果

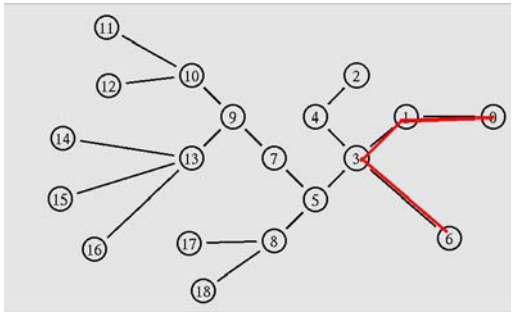
3.1.5 阻斷服務攻擊問題分析

當完成網路路由以及驛馬車問題後，成功說明了螞蟻搜尋最佳路徑的特性及精確性。而於阻斷服務攻擊問題中，我們採用了 3 個實例來做分析，此案例利用網路流量作為搜尋路徑的追溯來源。於圖 14 所示，節點數分別為 11、19、22 個節點以及網路流量不齊全之的網路路由來作模擬。如圖 14(a)所示，模擬 11 個節點為阻斷服務攻擊問題節點分佈圖，此範例利用流量作為搜尋路徑，我們，設定編號 0 為遭受攻擊的目標，而編號 10 號為發動攻擊之來源點，途中行經 3 個節點，阻斷服務攻擊路徑為 0-2-4-7-10。如圖 14(b)所示，模擬 19 個節點，設定編號 0 為遭受攻擊的目標，而與編號 0 相近的編號 6 設定為發動攻擊之來源點，途中行經 2 個節點，阻斷服務攻擊路徑為 0-1-3-6。如圖 14(c)所示，此實例模擬 22 個節點，設定編號 0 為遭受攻擊的目標，而編號 21 號為發動攻擊之來源點，途中行經 3 個節點，阻斷服務攻擊路徑為 0-3-10-11-21。

(a)



(b)



(c)

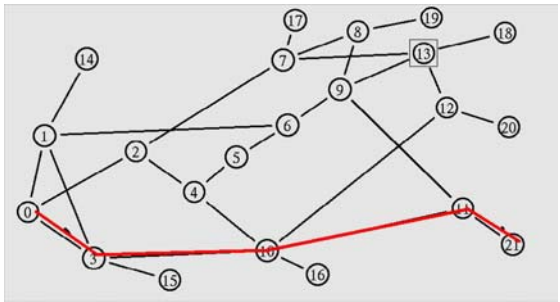
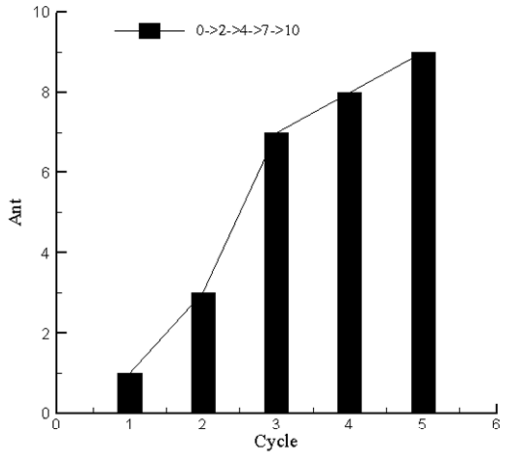


圖 14 阻斷服務攻擊問題搜尋模擬圖

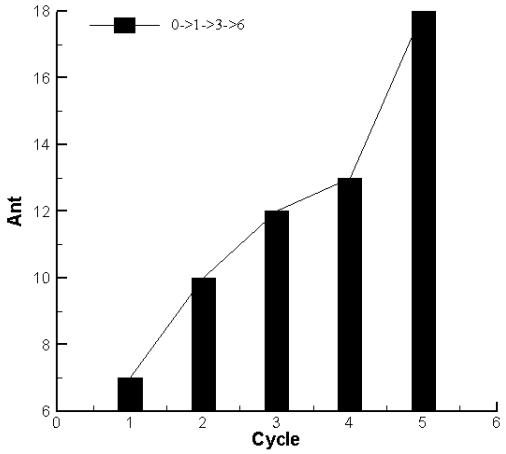
圖 15 為圖 14 之最佳路徑的螞蟻數量結果。如圖 15(a)所示，此範例為圖 14(a)之螞蟻數量結果圖，此案例係重複 Runs5 次並利用 11 隻螞蟻做為設定，最後求得具有近八成的螞蟻行經之阻斷服務攻擊路徑 0-2-4-7-10。如圖 15(b)所示，此範例為圖 14(b)之螞蟻數量結果圖，此案例係重複 Runs5 次並利用 19 隻螞蟻做為設定，最後求得具有多數的螞蟻行經之阻斷服務攻擊路徑 0-1-3-6。如圖 15(c)所示，此範例為圖 14(c)之螞蟻數量結果圖，此案例係重複 Runs10 次並利用 22 隻螞蟻做為設定，最後求得具有多數的螞蟻行經之阻斷服務攻擊路徑 0-3-10-11-21。

由以上三組實例所求得的結果如圖 15 所示，每一個最佳路徑的螞蟻數量均能在每一次的疊代中穩定成長，並能維持高比例的情況，由此顯現此螞蟻系統擁有良好的追溯阻斷服務攻擊的計算效能。

(a)



(b)



(c)

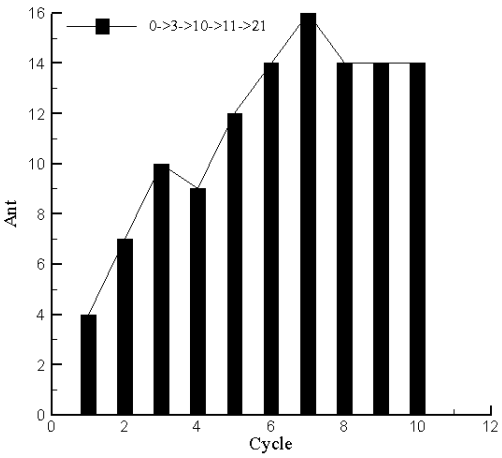
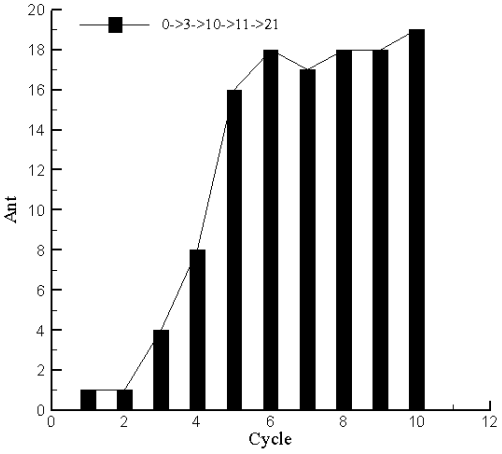


圖 15 阻斷服務攻擊問題之螞蟻數量結果

3.1.5.1 阻斷服務攻擊之網路流量不齊全問題分析

此問題探討圖 14(c)無法於一些路由器中完整取得網路流量資料的情形，如圖 16(a)所示，此範例無法於正常情況下取得節點 3 的網路流量資料，面對該問題，系統係重複 Runs 10 次並利用 22 隻螞蟻做為設定，並於節點 3 至節點 10 的網路流量設置為 0，結果顯示，最後仍可求得具有多數的螞蟻行經之阻斷服務攻擊路徑 0-3-10-11-21。如圖 16(b)所示，此範例為無法取得節點 10 的網路流量資料，系統係重複 Runs 10 次並利用 22 隻螞蟻做為設定，並於節點 10 至節點 11 的網路流量設置為 0，結果顯示最後仍可於資料不齊全的情況下，求得具有多數的螞蟻行經之阻斷服務攻擊路徑 0-3-10-11-21。

(a)



(b)

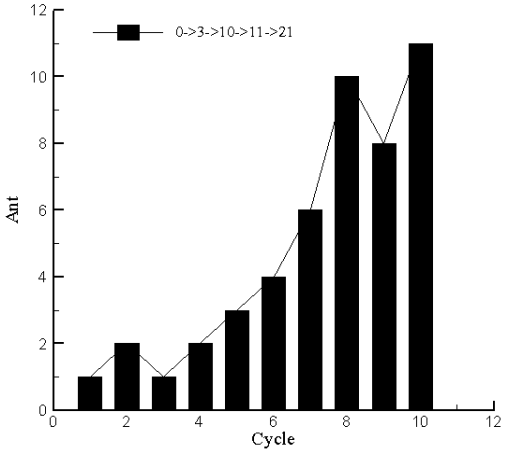


圖 16 阻斷服務攻擊之網路流量不齊全問題分析之螞蟻數量結果

3.1.6 大型阻斷服務攻擊問題分析

當完成以上三個小型阻斷服務攻擊與網路流量不齊全問題後，於該問題探討中，續將節點數增加至 41 個節點，進一步分析此系統於大型阻斷服務攻擊問題之精確性。

如圖 17 為阻斷服務攻擊問題模擬圖，我們模擬 41 個節點，由節點 0 開始為遭受攻擊的路由，直至節點 39 號為發動攻擊的來源點，途中僅行經 3 個節點，阻斷服務攻擊路徑為 0-22-3-18-39。

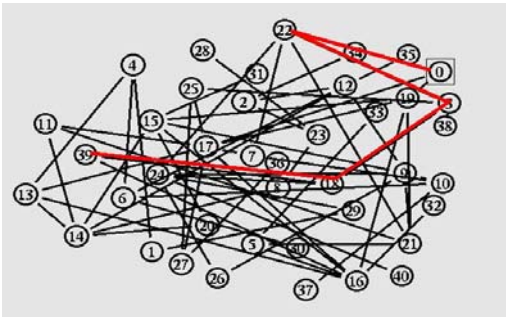


圖 17 阻斷服務攻擊問題搜尋模擬圖

如圖 18 所示，此系統係重複 Runs 10 次並利用 41 隻螞蟻做為設定，分別擺至各節點中。結果顯示蟻行演算法於 10 次疊代中即可快速達到收斂，且螞蟻數量均於每次疊代中穩定成長，並維持高比例之螞蟻數量，最後獲至最佳化的結果，由圖顯示具有近七成的螞蟻行經之阻斷服務攻擊路徑 0-22-3-18-39。

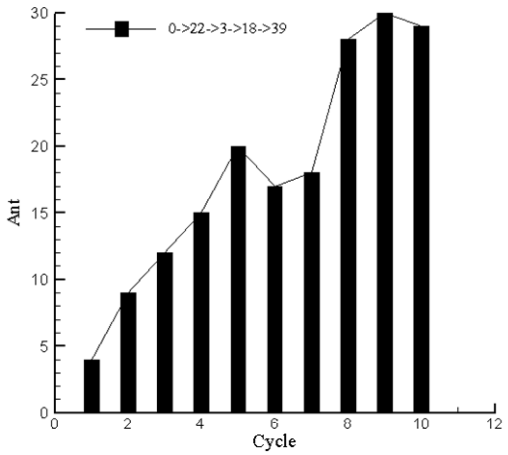


圖 18 阻斷服務攻擊問題之螞蟻數量結果

3.1.6.1 大型阻斷服務攻擊之網路流量不齊全問題分析

此範例為圖 17 案例中，無法於 router3 取得網路流量資料，此系統係重複 Runs 10 次並利用 41 隻螞蟻做為設定，並於節點 3 至節點 18 的網路流量設置為 0，其解如圖 19 所示，結果顯示最後仍可於資料不齊全的情況下，快速達到收斂，且螞蟻數量均能穩定成長，並維持高比例，求得具有多數的螞蟻行經之阻斷服務攻擊路徑 0-22-3-18-39。由此顯現此螞蟻系統擁有良好的追溯阻斷服務攻擊的計算效能。

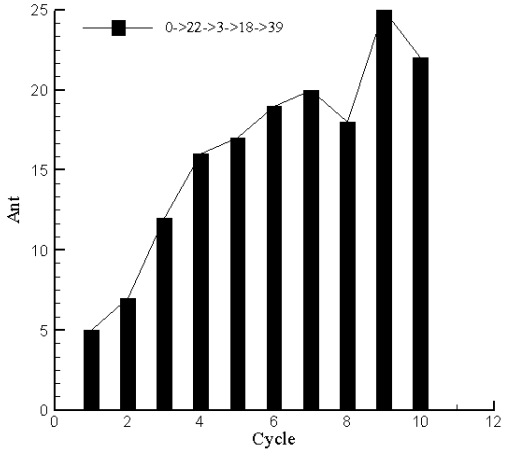


圖 19 阻斷服務攻擊問題之螞蟻數量結果

3. 結論

本文提出利用蟻行演算法求解最短路徑及網路攻擊來源，希望能夠藉由其獨特搜尋機制之特性來求得最佳路徑。在搜尋過程中螞蟻

以費洛蒙及網路攻擊流量(或距離)做為其搜尋路徑的機率值，其中費洛蒙之更新能夠有效的將前一疊代之解趨於最佳化。在追蹤阻斷服務攻擊範例中，即使在沒有完整攻擊流量之路由的情況下，無法以攻擊封包做判斷的同時，也均能善加利用費洛蒙的訊息來顯示出其搜尋之最佳解。而在所有搜尋路徑之問題中，螞蟻之搜尋疊代次數取決於節點數之多寡，相較於其他結果如 Berlin52 之疊代次數則開始需增加至 30 次以上之求解表現將有較高的顯著結果，其餘則無明顯差異。而阻斷服務攻擊問題中，雖以流量攻擊作為搜尋路徑的來源，結果顯示仍有同樣搜尋的效果，另一問題之網路流量不齊全問題分析中，雖於某些路由網路缺少流量資訊的情況下，亦能正確且有效率的找出該攻擊的來源位置，顯示螞蟻系統可在任何情況下搜尋出最佳的路徑。

參考文獻

[1] 李慶憲，網際網路攻擊來源回溯-分段式機率封包標記，***台灣商管與資訊研討會***，2006。

[2] 林尚逸，應用螞蟻演算法於基因篩選-以癌症分類為例，義守大學工業工程與管理學系碩士論文，2007。

[3] 柯志亨，計算機網路實驗:以 NS2 模擬工具實作，學貫圖書出版，2005。

[4] 馬淑珍，以網路流量資料探勘協助進行阻斷服務攻擊偵測與防禦之研究，國立中山大學資訊管理學系碩士論文，2005。

[5] 陳俊傑，以重疊網路防禦分散式阻斷服務攻擊，國立中央大學資訊工程研究所碩士論文，2005。

[6] 楊佳儒，以螞蟻演算法追蹤阻斷式服務攻擊來源之研究，國立中山大學資訊管理研究所，民國九十四年七月。

[7] 楊清然，在隨意無線網路上使用資料流管理對 VOIP 網路效能之改善方法，國立成功大學工學院工程管理碩士在職專班碩士論文，2007。

[8] 劉伯祥，劉仲祥，作業研究，全華科技圖書，2007。

[9] 劉杰宗，使用入侵偵測系統與流量控制模組減緩分散式阻斷服務攻擊，逢甲大學資訊工程學系碩士論文，2006。

[10] 劉振隆、杜宜蓉、蕭天輝、邱泰毓，演化式群蟻最佳化演算法應用於大型旅行銷售員問題，***資訊科技國際研討會***，2008。

[11] 鍾昌翰，適用於分散式阻斷服務與分散式掃描之網路入侵偵測方法，國立交通大學資訊工程學系，2001。

[12] Aljifri, H., Smets, M., and Pons A., "IP Traceback Using Header Compression," ***Computers & Security***, Vol.22, No.2, pp.136-151, 2003.

[13] Baba, T., and Matsuda, S., "Tracing Network Attacks to Their Source," ***IEEE Internet Computing***, Vol.6, No.3, pp.20-26, 2002.

[14] Computer Security Institute, "***CSI/FBI Computer Crime and security Survey***," 2003, http://www.crime-research.org/news/11.06.2004/423/ (accessed date: Dec. 20, 2008).

[15] Dittrich, D., The "Tribe Flood Network Distributed Denial of Service Attack Tool," http://staff.washington.edu/dittrich/misc/tfn.analysis (access date Jan. 12, 2009)

[16] Dorigo, M. and Gambardella, L.M., "Ant Colony System: A Cooperative Learning Approach to the Traveling Salesman Problem," ***IEEE Transactions on Evolutionary Computation***, Vol. 1, No. 1, 1997.

[17] Dorigo, M., Maniezzo, V. and Colorni, A., "The Ant System: Optimization by a colony of cooperating agents," ***IEEE/ACM Trans. On System, Man, and Cybernetics-Part B***, Vol.26, No.1, pp.1-13, 1996.

[18] Ferguson, P., and Senie, D., "Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing," ***RFC 2828***, 2000.

[19] Library of Traveling Salesman Problems Interdisciplinary Center for Scientific Computing, http://www.iwr.uni-heidelberg.de/groups/comopt/software/TSPLIB95/index.html (accessed date: Dec. 20, 2008).

[20] Mirkovic, J., "D-WARD:Source-End Defense Against Distributed Denial-of-Service Attacks," ***University California***, 2003.

[21] Park, K., and Lee, H., "On the Effectiveness of Probabilistic Packet Marking for IP Traceback Under Denial of Service Attack," ***Proc. IEEE INFOCOM***, Alaska USA, pp.338-347, 2001.

[22] Savage, S., Wetherall D., Karlin, A., and

Anderson, T., "Network Support for IP Traceback," ***IEEE/ACM Trans. Networking***, vol. 9, no. 3, pp.226-237, 2001.

[23] Savage, S., Wetherall, D., Karlin, A., and Anderson, T., "Network Support for IP Traceback, " ***IEEE/ACM Trans. Networking***, Vol.9, No.3, pp.226–237, 2001.

[24] Strayer, W.T., Jones, C.E., Tachakountio, F., Schwartz, B., Clements, R.C., Condell, M., and Partridge, C., "Traceback of Single IP Packets Using SPIE," ***Proc. DARPA information Survivability Conference and Exposition***, Vol.2, pp.266, 2003.

[25] The Network Simulator- ns-2, http://www.isi. edu/nsnam/ns/ (accessed date: Dec. 10, 2008).