管 理 與 系 統
第十六卷 第二期 民國九十八年四月
285-309 頁

Journal of Management & Systems
Vol. 16, No. 2, April 2009
pp. 285-309

網路誘捕系統之動態部署決策模式

The Dynamic Decision Model of Honeypot Deployment

王 平[1] Ping Wang
崑山科技大學資訊管理系

羅濟群[2] Chi-Chun Lo
國立交通大學資訊管理研究所

[1]Department of Information Management, Kun Shan University of Technology and
[2]Institute of Information Management, National Chiao Tung University

(Received August 5, 2007; Final Version January 30, 2008)

摘要： 近年來，資安組織成功運用入侵偵測系統 (Intrusion Detection System, IDS)，針對可疑的攻擊將其連線轉移至誘捕系統 (honeypot)，進行駭客或病毒的行爲觀察與分析，再將分析結果對所控管網路管理者發出警告，提供網路更堅實的保護。目前誘捕系統部署常運用「佈雷區」(minefield) 的策略，透過欺敵技術，將它們散佈網路上，以誘捕駭客；但常發現資訊蒐集的效果不彰，即使部署完成，常無法吸引攻擊者前來探測，造成誘捕系統形同虛設，故如何有效選擇部署節點，以期在最短時間內蒐集最多的網路攻擊資訊，並降低被駭客反偵測的可能性，是研究誘捕系統部署決策的重要議題。本研究運用機率與網路路徑分析技術，建立一個誘捕系統的動態部署分析數學模式，改進現有靜態佈雷區策略的缺失，改善誘捕系統之部署決策品質。面對部署效果不彰的問題，本研究分析在不同等級的網路服務品質 (Quality of Service, QoS) 限制下，運用最低成本法以分析駭客連線的最佳路徑，進而推估誘捕系統的最佳部署節點，以提高誘捕機率。系統驗證將以 NS2 (Network Simulator,version2) 工具模擬「隨機部署」、「最低成本部署」、「駭客擁有部份誘捕系統資訊下的部署」及「機動部署」等四種策略，由案例分析中，所提的決策模式，可有效協助網路管理者分析通訊網路中的建議部署節點及最佳部署節點。

* 感謝成功大學資通安全研究與教學中心 (TWISC@NCKU) 技術支援誘捕系統的安裝，此專案研究部份經費由國家科學委員會計劃編號 NSC 96-2219-E-006-009 及 NSC 96-2416-H -168-005 支援；此外，本文的審查委員所提的寶貴意見，促進內容的精進，在此一併表達謝意。

關鍵詞：誘捕系統、網路安全、最佳部署、佈雷區

Abstract: To effectively provide an early alarm of dangers for attack events, security organizations have successfully employed Intrusion Detection System (IDS) to transfer the suspicious connections to honeypot which can capture and analyze the hacker's behavior and virus signature for years. Using the minefield strategy to deploy honeypot systems, managers place decoy systems and spread them among network nodes to trap hackers. There exists the problem that honeypot constantly cannot appeal the attention of hacker's attack if honeypot is deployed within the inappropriate zone or node. It is a crucial issue that how to effectively deploy it for accumulating large numbers of information as well as decrease the anti-detect possibilities by hackers. Hence, we develop a network-based analysis model for dynamic honeypot deployment through the use of probability theorem and traffic analysis technique to improve the limitations of way of static strategy, promote the decision quality of honeypot deployment. It discovers the best route with the minimum cost, and decides the optimal deployment node to increase the trap possibility within distinct QoS constraints. Using NS2, this model is validated by four network deployment strategies, that is, minimum-cost deployment, random deployment, Bayes-based deployment and dynamic deployment, to test its efficiency. The experimental results show that the proposed approach can effectively locate the recommended nodes and the optimal node of honeypot deployment in a communication network.

Keywords: Honeypot, Network Security, Optimal Deployment, Minefield

1. 前言

隨著網路技術演變，各種網路應用便利我們的生活，但隨之而來的網路安全事件的危害也越來越嚴重。傳統的資訊安全管理技巧，主要是透過系統弱點偵測作資訊系統體檢，以防火牆阻擋未授權的存取，運用入侵偵測系統作攻擊偵測，但這些技術都常無法有效防範駭客的攻擊。解決之道是在於網路上佈署誘捕系統，藉由預設的漏洞吸引入侵者，蒐集與分析駭客與病毒的特徵，瞭解敵人，將其行爲特徵建入侵偵測系統的偵測規則中，當網路發生攻擊時，才能及時提供入侵者手法和相關資訊，以預定的措施保護資訊系統 (賽門鐵克研究實驗室，民 94)。

近年來資安組織成功運用入侵偵測系統 (Intrusion Detection System, IDS)，針對可疑的攻擊將其連線轉移至誘捕系統 (honeypot)，進行駭客或病毒的行爲觀察與分析，將分析結果對所控管網路管理者發出警告，提供網路了更堅實的保護。但誘捕系統亦存在某些特徵，容易被駭客識

別，甚至被佔領 (compromised)，本身可能被攻擊者作爲另外一次攻擊的跳板，因此誘捕系統的部署策略，須考量週遭環境特徵，適當的掩飾身份，降低被反偵測的機率。通常誘捕系統是指單一主機模擬網路的各種服務，而誘捕網路系統 (honeynet) 則是採用真實的網路系統，這一網路系統是隱藏在防火牆後面，所有進出的資料連線都受到監控、捕獲及控制 (Honeynet Project, 2001)。誘捕網路系統是一個很有價值的資安研究環境，目前成大資通安全研究與教學中心 (TWISC@NCKU) 已完成誘捕網路系統的建置，學者可利用這個公開的平台，誘捕各種網路攻擊事件，深入了解入侵者手法或病毒攻擊方式，以便未來能及早偵測或重現 (replay) 網路的攻擊模式。

許多知名的網路安全組織，如綠盟、ISS 等均部署誘捕系統，作爲收集情報及統計數據的工具，但發現駭客發展工具，反偵測誘捕網路系統並進行破壞，例如 Dornseif *et al*. (2004) 提出數種方法並發展出偵測工具，成功偵測誘捕網路系統的資訊擷取工具－Sebek，並使 Sebek 失去效用。此外，Keong (2004) 亦發展出微軟視窗作業系統的 Sebek，以保護及偵測入侵，這一場資安人員與駭客間的作戰已進入攻防循環之中。如何擬定一個有效的部署策略，反制駭客對已部署的誘捕網路系統反偵測及破壞，是一個重要且值得探討的議題。

現行的誘捕系統部署策略有兩種:佈雷區 (minefield)：將誘捕系統散佈網路上，與真實的伺服器交錯安置，混淆駭客的注意，伺機加以誘捕，但常發現靜態佈雷區對資訊蒐集的效果不彰，即使部署完成，常無法吸引攻擊者前來探測，使部份誘捕系統形同虛設；防護罩(shield)：在每一上線服務伺服器均對應一個誘捕系統，有如請一位保鏢 (bodyguard) 來保護重要主機，可將進出伺服器的異常通訊連線，指向對應的誘捕系統來處理。這種過濾可疑的轉移連線的方法，很容易被精明的駭客發覺，因此發展一個不須轉移連線的部署方法是目前發展的重要趨勢 (Hernacki *et al*., 2004；賽門鐵克研究實驗室，民 94)。基於上述理由，本研究改進靜態佈雷區的缺點，建立一個『誘捕系統動態部署決策模式』，其目的爲發展一個不須轉移連線的策略，透過動態部署策略，達到降低被駭客反偵測的可能性，透過最佳部署節點的選擇，提高誘捕機率，改善誘捕系統之部署決策品質。

第 2 節文獻探討誘捕系統部署的相關研究，第 3 節推導部署決策模式，第 4 節列舉實例說明，進行四種部署策略及與其他方法的比較分析，第 5 節作出結論及建議未來研究方向。

2. 文獻探討

已有數位學者研究誘捕系統部署的相關問題，重要的研究包括: Gupta（2003）認爲將誘捕系統部署於網路流量過低之網路節點，則將無法蒐集攻擊資訊，這是目前誘捕系統部署遭遇到的常見問題。McMullen（2004）建議將誘捕系統部署在防火牆與非交戰區 (De-Militarized Zone,

DMZ)，此方法可誘導攻擊者掉入誘捕系統，提升內、外部網路的安全層級。Pelletier（2004）建議誘捕系統必須設置在真實的網路上，部署節點可選在內部網路或非交戰區，以監控來自企業內、外部的攻擊。此外，Cohen and Associates（1998）嘗試以網路拓樸 (topology) 架構，分析誘捕系統的部署方法，在應用系統間設置預設系統弱點 (vulnerabilities) 的誘捕系統，吸引攻擊者入侵系統，但因命中機率 (hit probability) 太低，進而發展一套欺敵與部署的工具軟體－DTK (Deception Toolkit)，運用多址 (multi- home) 技術，以一個主機模擬多個誘捕系統，散佈於眾多真實系統間，以提高誘捕機率。研發誘捕系統的先驅 Lance 則提出兩個誘捕系統部署的新觀念：機動式誘捕系統 (dynamic honeypot) 與誘捕系統莊園 (honeypot farm)；前者強調分散式部署，後者重視集中式管理。機動誘捕系統爲一隨插即用 (plug-and-play) 部署方法，藉由自動化計算部署數量，如何僞裝並與現有環境相契合，降低被反偵測的可能性。「誘捕系統莊園」的觀念則是捨棄大量部署的想法，透過部署簡易的偵測器，類似派出哨兵，若發現可疑連線，則轉移至堅固防護的誘捕系統莊園 (Lance, 2003a; Lance, 2003b)。部份學者已針對上述兩個新觀念進行實做，例如 Sherif *et al*. (2004) 實做活動式的誘捕系統 (roaming honeypot) 部署方式，以對抗分散式阻斷服務攻擊。Chen *et al*. (2005) 實做並於臺灣先進學術網路上部署誘捕系統，分析網路的駭客與病毒行爲特徵。上述的研究，均是採用隨機部署，並未針對現有的佈雷區、防護罩及機動式部署策略，分析駭客最可能出現的路徑及可能落入誘捕系統的機率，亦無說明最佳部署節點爲何。

3. 部署決策模式的建立

3.1 部署策略的探討

今日的資安科技無法提供絕對資訊安全防護，故資訊「僞裝」與「欺敵」應是防衛我重要資訊基礎建設的重要手段，故在制定部署誘捕系統的部署策略時，須考慮部署的有效性及降低被反偵測的機率，以提高系統的安全性。

3.1.1 初步想法

誘捕系統應用於網路欺敵手法，可歸納「僞裝」與「誘敵」兩種技巧。「僞裝」是爲了降低被駭客偵測的機率，而「誘敵」則爲引誘駭客進入，透過試探認識駭客的攻擊手法，兩種方法可交互運用，以擴大網路欺敵的效果。

僞裝技巧就是俗話的「隱身」，在現代網路作戰的常用的僞裝手法，包括(1)減少暴露行縱，如隱形飛機降低紅外線的排放量，潛水艇降低噪音，以減少被偵測的機率；誘捕系統則是將相關目錄、登錄檔 (registry)、程序名稱，對外連線傳送系統記錄加以隱藏；(2)僞裝成與背景相似的物件，將誘捕系統僞裝成現實世界中有缺陷的物件，其特徵與週遭的物件相仿，仿如是系統

中的一員，例如在電子商務系統中，將誘捕系統僞裝成電子郵件系統。因爲網路環境是動態的，過時的作業系統版本，將與週遭的環境格格不入，提高被反偵測的機率；因此，發展誘捕系統的部署策略，須考量僞裝技巧，將誘捕系統部署於正常的電腦群中，以週遭環境掩飾身份，降低被反偵測的機率。

運用誘捕系統於網路欺敵，實作技術上有三個重點：(1)誘捕系統漏洞佈置－我們必需先推估駭客可能攻擊的目標，才能在誘捕系統適當設定漏洞，引誘敵人；(2)誘捕系統參數的設定－系統參數決定誘捕系統的特徵，如何將誘捕系統的特徵降至最低，躲避駭客的偵測；(3)誘捕系統的測試－先以弱點偵測系統掃瞄誘捕系統，是否查出預設的漏洞，但無法辨識此系統就是誘捕系統。 當蒐集到資料，可將駭客編號與建檔，熟悉駭客的技巧，分析駭客的動機，因爲在網路攻防上，了解攻擊者行爲、主要的目標及動機是非常重要的 (Cohen, 2000; Gupta, 2002; Hernacki *et al*., 2004)。在孫子兵法的「虛實篇」提到兩個與網路欺敵相似的攻防技巧：

(1)「能使敵人自至者，利之也」－意思就是使用小利引誘，就能夠使敵人自動進入我預定的領域，並誘使其主動對誘捕系統發動攻擊，讓我們取得其攻擊手法，來加以分析及了解攻擊者的攻擊程序及技巧。當然我們必需設定基本的漏洞，才能使吸引攻擊者的注意，引誘攻擊者進入，就像孫子所題出的要攻擊敵人弱點的道理一樣，因爲一般攻擊者並不會對無弱點或安全性等級較高的電腦感興趣。

雖然此方法有著不錯的基本假設理論，但是若太過於大意，任意讓攻擊者任意攻擊，卻極有可能造成系統被佔領而成爲殭屍電腦 (zombie)，當作另一攻擊的跳板。所以在「誘捕系統」設定上，不單只是考量到如何引誘攻擊者進入攻擊系統弱點的問題，須考量如何讓攻擊者容易進入系統，但不輕易的離開，擷取到攻擊者的手法才是重點。當攻擊者在進入系統的同時，我們可以設置更難突破的系統，讓攻擊者不輕易完成所要做的攻擊動作，除了可以延長攻擊者在系統裡的時間外，更可以在攻防間取得平衡，而不讓攻擊者發現系統的真僞。

(2)「故策之而得失之計，作之而知動靜之理，形之而知死生之地，角之而之有餘不足之處」－意思就是通過認真的籌算，分析敵人作戰計畫的優劣勢得失；透過挑逗敵人，來增加瞭解敵人的活動規律；通過佯動示形，來試探敵人弱點所在；透過與對手交鋒，來瞭解敵人兵力的虛實與強弱 (普穎華, 民 94)。

3.1.2 部署策略的進一步探討

誘捕網路系統運用一個網路系統，以進行誘捕非法的連線，其通常被部署在防火牆後面，透過特定功能的防火牆 (honeywall) 監控、捕獲及控制所有進出的資料連線，亦可以單一主機模擬網路上的各種服務，即爲虛擬誘捕系統 (virtual honeypot)，其示意圖如圖 1。

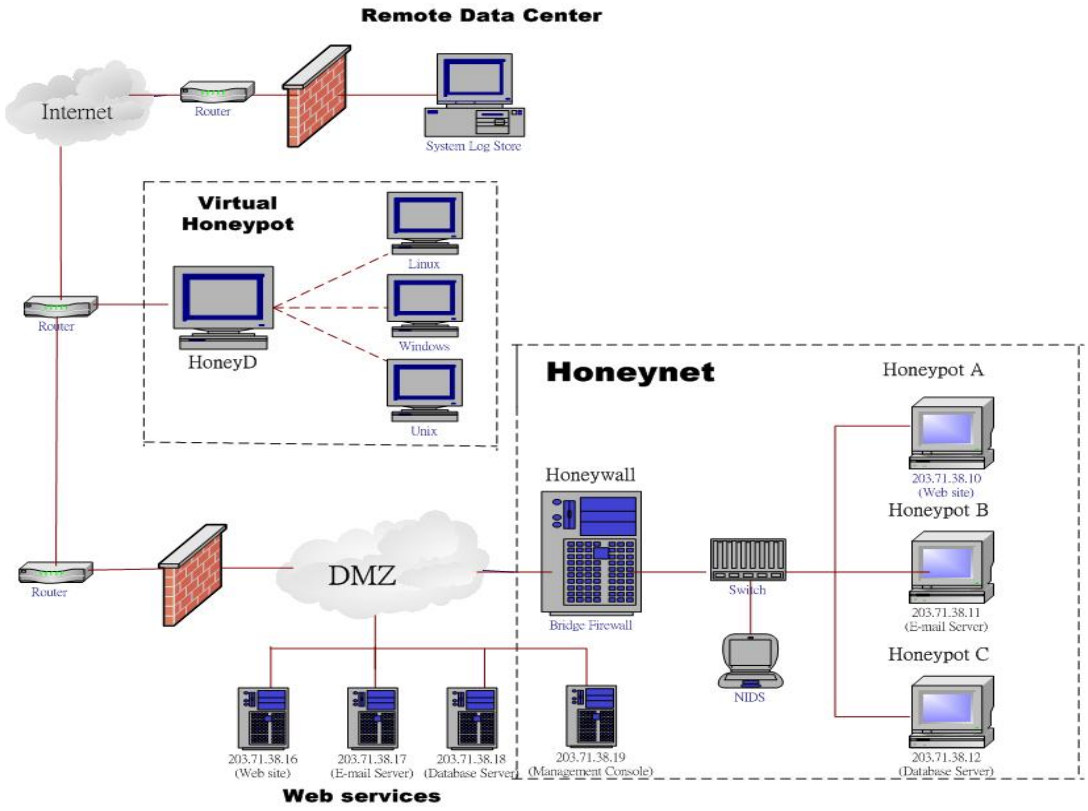

圖 1　誘捕系統架構的示意圖

若以允許攻擊者的活動層級而言，誘捕系統又可區分爲兩種互動 (interaction) 模式：(1)低互動誘捕系統: 系統提供有限的活動，藉由模擬服務與作業系統來運作。其主要優勢在於比較容易部署與維護，風險也比較小，因爲攻擊者絕不會進到一個真正的作業系統及應用程式，而達到傷害其他系統的目的。常見的低互動式誘捕系統如－ “HoneyD”，其主要的功能是監控連線狀況及沒有使用的網路位址空間；(2)高互動誘捕系統: 系統的活動牽涉到真正的作業系統與應用程式，而不是模擬服務方式。提供攻擊者真實的系統來進行互動，以收集到更多關於攻擊者的知識。高互動系統優點是彈性靈活，但是由於攻擊者可能利用此系統上發動攻擊，因此在這類誘捕系統的建置上，需要付出額外的技術與風險 (黃志雄、王智弘，民 93)。

以下針對 Hernacki *et al*. (2004) 提出佈雷區及防護罩兩種部署策略及 Sherif *et al*. (2004) 提出機動式的誘捕系統概念，加入實做方法，說明如下：

(1) 佈雷區的部署策略

佈雷區的部署策略是採用誘捕系統與真實的伺服器相互安插，混淆駭客的注意，示意圖如圖 2。誘捕系統常部署在非交戰區區域中的伺服器，主要捕捉來自外部網路的攻擊。早期誘捕系

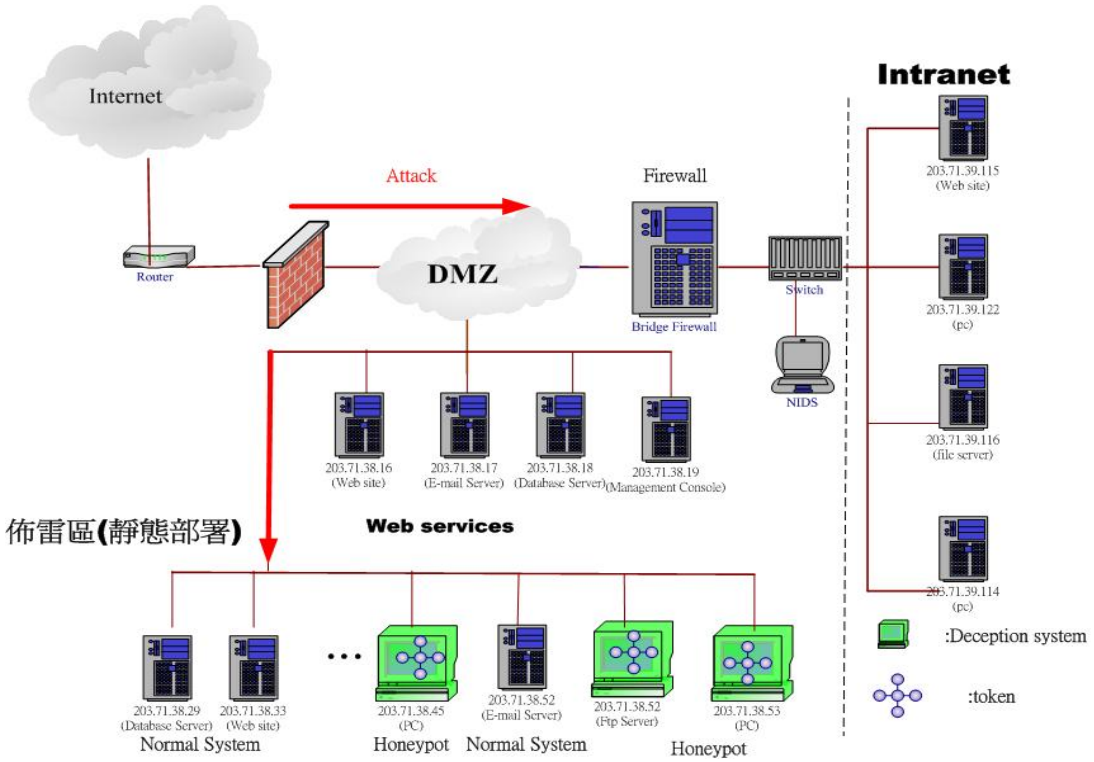

圖 2　佈雷區部署策略

統採用預設少量的系統弱點，以吸引入侵者進入，主要挑戰來自如何引起駭客的注意，透過防火牆將可疑連線轉移，但此種方式很容易被入侵者反制及查覺。後來，因預設單點的系統弱點的方式，並不易引起入侵者的注意，另一種可廣泛與系統服務結合的誘捕系統－網路欺敵工具 DTK 被研發出來，以解決上述問題 (Cohen, 1998)。它具有兩種功效：(1)其運用多址 (multiple home/ address) 技術，可將誘捕裝置部署於大量的網路位址空間，(2)以智慧探測 (intelligence probe) 取代以系統弱點來吸引入侵者，大幅增加欺敵機率。

值得一提的是網路欺敵工具 DTK 在網路欺敵使用上仍有一些限制：(1)目前尚無法運用精確數學理論，搜尋可用空間中，作出完整的智慧探測與部署，(2)因爲大量部署誘捕裝置，故常無法兼顧到網路欺敵的效用。其仍存在一些系統缺失，只能在一定網路範圍內刺探入侵者，無法大範圍部署使用。但當入侵者比管理者擁有更多先進探測能力時，網路欺敵工具通常無法影響對方的作爲。針對上述缺失，Cohen (2000) 研究網路欺敵方法，探討網路欺敵的作法與系統架構，其建議結合路徑轉移 (rerouting) 與真實系統的搭配模式，可達成最真實的欺敵效果。他提出以加大位址空間及僞裝誘捕系統，改善 DTK 的偵測能力的解決方法，以提高部署的有效性及降低被駭客反偵測的機率：

(1)一址多戶 (multi-home in a box)； (2)多址解決方案 (multiple addresses resolution)，透過多址技術，最高可模擬產生達 64,000 網路位置，作爲虛擬的誘捕系統，並將此命名爲欺敵牆 (Deception Wall, D-WALL)。 D-WALL 與 DTK 的不同點是: 前者是增加部署誘捕裝置於網路位址空間，還提供了設計細緻的系統漏洞，進一步引誘入侵者一探究竟；而後者則是只是增加更多的誘捕裝置。因爲目前主機刺探掃描工具會針對一整段的網路位址作掃描，使欺敵牆很快偵測到入侵行爲。駭客攻擊很少會只限於單一電腦上，許多自動化的網路攻擊都遵循同樣的模式，假定網路中的一台電腦已經被成功的攻擊，則這台電腦接著會被作爲殭屍電腦，繼續用來掃描網路上其它潛在的目標，以利後續的攻擊，因此欺敵牆可有效攔截到網路的非法掃瞄，並引誘入侵者作出攻擊。

(2) 防護罩的部署策略

雖然誘捕網路系統能有效蒐集駭客攻擊資訊，但在資訊蒐集與環境風險須取得折衷 (compromises)，否則本身可能作爲攻擊者另外一次攻擊的跳板，因爲誘捕系統存在弱點且容易爲駭客所利用，以修改稽核記錄(log)及破壞作業系統的資料，故網管人員聯想到以防護罩的觀念進行誘捕駭客；防護罩的部署策略是在每一上線服務伺服器均對應一個 誘捕系統，有如請一位保鏢來保護重要主機，可將進出伺服器的異常通訊連線，指向對應的誘捕系統防護主機來處理。這個架構需要有個路由器與防火牆，根據目的連接埠以防火牆來過濾網路通訊，然後根據防護罩政策來做通訊轉向，過濾可疑的連線。以圖 3 防護罩的誘捕裝置的部署策略爲例，部署在非交戰區的三台網路伺服器來說明，任何伺服器通訊中合法的連線被導引至伺服器，但發生可疑的連線，防火牆會將此連線指向誘捕系統，並將來源端的位址加以記錄。

若要提高誘捕系統的效用，可以複製所防護的伺服器部分或全部非機密內容到誘捕系統，以欺騙駭客，認爲其仍然在伺服器中。進一步的觀念延伸是，針對重要主機保護，亦可以一群保鏢來保護它，形成多層的防護，加強其資訊安全的防禦縱深 (in-depth defense)，以免造成駭客突穿 (penetration)，產生資訊安全的致命漏洞。防護罩的網路部署系統的架構，須組合資安設備，例如系統弱點掃瞄、誘捕系統、防火牆與路由器，以偵測潛在的攻擊，運用 誘捕系統代替實際的攻擊目標做出預設的回應，緊急時可中斷對外連線 (outbound connections)，預防致命及後續的攻擊，確保主機不被佔領。因爲營運中的伺服器通常只需要開放少數幾個連接埠，將對應的連接埠引導一個受攻擊連線，直接通往誘捕系統以利蒐證及分析攻擊的行動。防護罩部署可作爲重要主機系統的保護，例如資料庫主機，因爲攻擊最可能發生在組織中重要的主機系統。

3.2 動態部署策略

本研究的部署策略是延伸佈雷區的方法，將靜態的部署改爲動態方式，強化其理論基礎，以大量的陷阱誘捕入侵者，搭配機動位置變換，運用機率與網路路徑分析 (routing analysis) 理

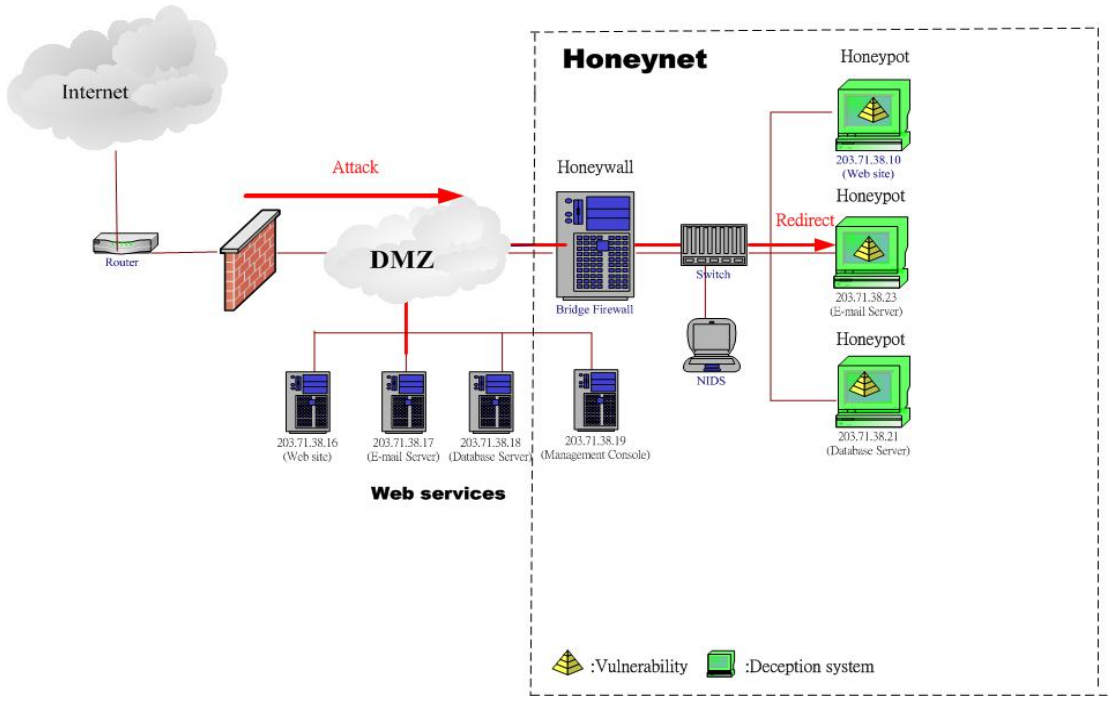

圖 3　防護罩部署策略

論，將此問題視爲一個網路應用的機率決策問題，透過貝式決策準則 (Baye's decision criterion)，分析「隨機部署」、「最低成本部署策略」、「駭客擁有部份誘捕系統資訊之事後機率 (posterior probability) 部署」及「機動部署」四種部署策略，輔助管理者作出部署決策，反制駭客的偵測，增加誘捕系統的存活率，詳細說明如下：

(1) 策略 I：隨機部署策略

在某個網段 (network subnet) 中，在 200 台伺服器部署 50 個誘捕系統，假設駭客利用隨機單點攻擊，駭客落入誘捕系統的機率是 20%，其運算公式爲:

$$P_h = N_h / (N_r + N_h) \tag{16}$$

其中 P_h 爲落入誘捕系統的機率 (hit probability)，N_r 爲此網段中真實系統的數目，N_h 爲此網段中誘捕系統的數目。

(2) 策略 II：最低成本部署策略

首先，對誘捕系統部署節點分析模式的建立說明如下:假設網路流爲一非循環的有向圖，因爲循環的有向圖中，頂點 (vertices) 間將可能會連接無限多個路徑 (paths)，造成不易分析。針對網路路徑的建構，分析的問題包括：(1)任意兩頂點間連通的路徑數目爲何，(2)最佳部署節點

的選擇。首先，假設通訊網路中的路由器，以動態選擇最低成本爲其繞送路徑，以降低傳輸成本。令網路的拓樸可表示爲一有向圖 $G=(V,E)$，其中網路的頂點集合 (頂點在網路術語爲節點，故以下均採用節點描述)爲 $V=\{v_1, v_2,\ldots, v_n\}$, V_s 代表源點 (sources) 的集合，V_d 代表匯點 (sinks) 的集合，E 爲圖形的邊 (edge)，本研究將誘捕系統最佳部署節點的分析，說明如下:

步驟 1：決定兩頂點間 (源點至匯點) 連通的路徑數目

以相鄰矩陣 (adjacent matrix) $M=\{v_{ij} \mid i=1,..,m; j=1,...,n\}$ 來代表圖形的邊 E，依據 Skvarcius and Robinson (1986) 所提的兩端點的路徑分析定理 6.4 可知，相鄰矩陣 M 的冪次方(power)，M^* 爲 M 的其他冪次方的或(or)組合

$$M^* = M^1 or M^2 or M^3 or ... or M^p \tag{1}$$

其中 M^* 代表有向圖的可達性矩陣 (reachability matrix)，從 M^* 可分析從 v_i 到 v_j 的路徑是否存在路徑，例如 M^* 代表 v_1 到 v_2 不存在路徑，但 v_1 到 v_3 存在路徑。

$$M^* = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \tag{2}$$

其中 $M^2 = M * M, M^3 = M^2 * M,$ 依此類推。

接下來，計算 m 個源點至 n 個匯點間的連接路徑數，定義計算連接路徑數矩陣 $N(i,j)$，矩陣的元素代表爲一節點 i 至節點 j，路徑長度爲 1 的個數

$$N(i,j) = \begin{cases} 0 & , \quad if(v_i, v_j) \notin E \\ 1 & , \quad if(v_i, v_j) \in E \end{cases} \tag{3}$$

再運用歸納法可由得節點 i 至節點 j，路徑長度爲 k 的路徑個數。首先定義 $N(i,j)$ 的冪次方爲 $N_k(i,j)$，可透過先前矩陣乘積來計算。例如 N_1 爲一個 mxp 矩陣(經過 p 個中間點)，元素內容定義如方程式(3)，N_2 爲一個 pxn 矩陣，則此有向圖的兩頂點間的路徑數目，可運用關係的合成如圖 4。

基於 N_1x N_2 成爲 mxp 矩陣，N_3 矩陣可表示爲

$$N_3(i,j) = \sum_{k=1}^{p} N_1(i,k).N_2(k,j) \tag{4}$$

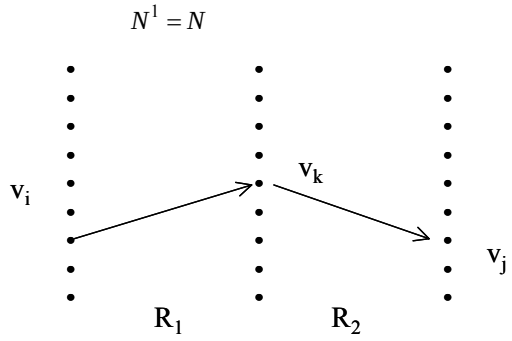

圖 4 有向圖的兩頂點的路徑數目計算示意圖 (Skvarcius and Robinson, 1986)

運用歸納法，以矩陣 N^k 計算出兩端點間路徑長度爲 k 的可能路徑個數

$$N^1 = N$$
$$N^k = N \times N^{k-1} \qquad \forall k \geq 2. \tag{5}$$

步驟 2：計算最低成本路徑及部署的最佳節點

根據網路基準測試 *RFC2544* 所定的網路服務品質參數，包括頻寬、延遲度、抖動和丟包率…等指標。而實務上常以頻寬 (Bandwidth, BW)、延遲度 **(**Delay**)** 及與網路設備的穩定度 (Stability, 抖動和丟包率) 做爲參數設定。假設路由器繞送 (routing) 是以網路服務品質爲依據，則網路傳輸成本與網路頻寬成反比，與網路設備的穩定度成反比，但與網路壅塞程度所造成的傳輸延遲成正比。假設頻寬、延遲度及與網路設備的穩定度三者爲相互獨立的變數，以簡化藕和 (coupling) 效應及避免非線性模式的參數估算 (parameter estimation)，故節點 i 與節點 j 間的網路傳輸成本評估函數(c_{ij})設爲三項 QoS 參數的線性組合如下

$$c_{ij} = RBW_{ij} + RST_{ij} + DL_{ij} \tag{6}$$

其中 RBW_{ij} 代表節點 i 與節點 j 間的頻寬的倒數， RST_{ij} 代表穩定度的倒數， DL_{ij} 代表傳輸延遲度，其中頻寬、延遲度及穩定度因單位不同，需先經正規化 (normalization)，首先將網路傳輸成本劃分十個等級，再運用等差級數 (1.0, 0.9,…0.1,0.0) 給予相對應傳輸成本，依據「網路傳輸成本評估函數」，選擇最小成本作爲傳輸節點；首先列出連接兩節點的邊 E 的相鄰矩陣 (adjacent matrix)，針對每一源節點計算至下一節點的網路傳輸成本，選出最低成本的節點作爲連接節點，直到匯節點爲止，即完成一條最低成本路徑 (Minimum-Cost Path, MCP)，故 m 個源點至 n 個匯點間共存在 mxn 條最低成本路徑，其數學分析模式爲

$$
\begin{aligned}
&Min \qquad \sum_{(i,j\in E)} c_{ij} v_{ij} \\
&subject \quad to \quad c_{ij} = RBW_{ij} + RST_{ij} + DL_{ij}, \\
&\qquad 0 \le RBW_{ij} \le 1, \ 1 \le i \le m, \ \ 1 \le j \le n \\
&\qquad 0 \le RST_{ij} \le 1, \ 1 \le i \le m, \ \ 1 \le j \le n \\
&\qquad 0 \le DL_{ij} \le 1, \ 1 \le i \le m, \ \ 1 \le j \le n \\
&\qquad v_{ij} \in \{0,1\}.
\end{aligned} \tag{7}
$$

其中 v_{ij} 代表兩節點間的連線狀態，v_{ij}=1 爲兩節點間爲連線 (connected)，反之 v_{ij}=0 代表兩節點間爲斷線 (disconnected)。決策變數爲 v_{ij}，比較 v_i 相連節點的傳輸成本，當節點 v_j 被選爲最低成本路徑中的節點則 v_{ij}=1，反之 v_{ij}=0。最低成本路徑中的節點連接，可利用線性規劃求解。最低成本路徑可表示爲節點的集合 $MCP = (v_i, ..., v_j)$ ，假設共有 r 條最低成本路徑經過節點 v_k，則針對 r 條最低成本路徑，計算經過節點 v_k 的傳輸成本總和 $TC_{ij}(v_k)$ 爲

$$
TC_{ij}(v_k) = \sum_{k=1}^{r} c_{ij}(v_k), \quad v_k \in MCP \tag{8}
$$

其中 $c_{ij}(v_k)$ 爲單一最佳路徑經過節點 v_k 的傳輸成本。比較各節點(除 m 個源點及 n 個匯點外) 傳輸成本總和，選擇最低傳輸成本者，建議爲誘捕系統部署的最佳節點 $D_{opt}(v_k)$

$$
D_{opt}(v_k) = \underset{k \notin V_s, V_d}{Min} (TC_{ij}(v_k)) \tag{9}
$$

因假設路由器以動態選擇最低成本者，作爲繞送路徑，故最佳路徑爲攻擊者最可能經過的路徑，若流經節點 v_k 的總成本最低，可推測經過的相對次數 (機率函數的密度) 爲最高，期望可於最短時間內取得最多的攻擊次數，故選爲誘捕系統的最佳部署節點。

(3) 策略 III: 已知駭客擁有部份誘捕系統資訊下的部署策略

因爲目前駭客已完成發展反偵測誘捕網路系統工具，並將其所反偵測到的資訊公佈在駭客的網站上，以規避誘捕系統的追蹤。故在分析駭客落入誘捕系統的機率時，須將駭客可能擁有情報資訊的狀況 (X) 納入考慮，其落入誘捕系統的機率 P_h 須修正爲 $P_h(S_i|X)$，其中 S_i, i=1,…,n，S_i,表示各種狀況 (states)，包括落入誘捕系統的狀況或落入真實系統的狀況，此運算公式爲一事後機率 (posterior probability)。很明顯的，增加誘捕系統的數量 (N_h) 將提高 $P_h(S_i)$，i=落入誘捕系統的狀況，或降低駭客擁有誘捕系統的情報機率 $P_h(X)$，亦可提高駭客落入誘捕系統的條件機

率。因考量駭客攻擊前可能已擁有或無情報資訊的狀況，故可透過貝式決策準則分析駭客落入誘捕系統的機率如下：

$$P_h(S_i \mid X) = \frac{P_h(X \mid S_i) * P_h(S_i)}{\sum_{i=1}^{n} P_h(X \mid S_i) * P_h(S_i)} = \frac{P_h(X \mid S_i) * P_h(S_i)}{P_h(X)}, \tag{10}$$

其中 $P_h(S_i|X)$ 爲利用情報資訊 X，修正駭客落入誘捕系統的條件機率，$P_h(S_i)$爲發生狀況 S_i 的機率，屬於事前機率，$P_h(X|S_i)$則爲發生駭客落入誘捕系統或真實系統的狀況下(S_i)，事先駭客擁有情報資訊 (X)的機率，其數值視狀況 i 而定，i=1 落入誘捕系統的狀況；i=2 落入真實系統的狀況。舉例說明如表 1。

我們有興趣的是駭客擁有情報資訊的機率(X_1)，駭客落入誘捕系統的條件機率值 $P_h(S_1 \mid X_1)$ 爲

$$P_h(S_1 \mid X_1) = \frac{P_h(X_1 \mid S_1) * P_h(S_1)}{\sum_{i=1}^{2} P_h(X_1 \mid S_i) * P_h(S_i)} = \frac{P_h(X_1 \mid S_1) * P_h(S_1)}{P_h(X_1 \mid S_1) * P_h(S_1) + P_h(X_2 \mid S_2) * P_h(S_2)} = \frac{0.2 * 0.6}{0.2 * 0.6 + 0.6 * 1.4} = 0.125.$$

同理可求出駭客擁有情報資訊的機率(X_1)的狀況下，駭客落入真實系統的條件機率值 $P_h(S_2 \mid X_1)$ 爲 0.875。假設運用誘捕系統截取駭客連線的效用如表 2。部署誘捕系統且採用某一行動方案(A_k)的預期效用值 (Expected Utility, EU) $EU(A_k)$ 爲

表 1　駭客落入誘捕系統的條件機率值

假設條件	發生狀況	
	落入誘捕系統的狀況(S_1)	落入真實系統(S_2)
駭客擁有情報資訊的機率(X_1)	**0.2**	**0.8**
駭客無情報資訊的機率(X_2)	**0.4**	**0.6**

表 2　誘捕系統的效用

行動方案	發生狀況	
	落入誘捕系統的狀況(S_1)	落入真實系統(S_2)
截獲少量但價值低的駭客資訊(A_1)	**0.8**	**0.1**
截獲部份有價值的駭客資訊(A_2)	**2.4**	**0.2**
截獲完整有價值的駭客資訊(A_3)	**7.6**	**0.5**

$$EU(A_k)=\sum_{i=1}^{n} R_{ki} * P_h(S_i), \tag{11}$$

其中 R_{ki} 爲在狀況 S_i 下，採用某一行動方案(A_k)，產出的報酬值 (return)。以截獲完整有價值的駭客資訊的行動方案 A_3 爲例，若發生 $P_h(S_1)$=(0.4+0.2)/((0.4+0.2)+(0.8+0.6))=0.3，發生機率 $P_h(S_2)$=1-0.3=0.7，則預期效用值爲 $EU(A_3)$=7.6*0.3+0.5*0.7=2.63。

同理可求出其他行動方案的預期效用值 $EU(A_1)$=0.31，$EU(A_2)$=0.86，很明顯 $EU(A_3)>EU(A_2)>EU(A_1)$。

(4) 策略Ⅳ：機動部署策略

若選擇誘捕系統部署是固定的網址，駭客可能以探測工具找到部署的位置。故本研究提出機動部署策略，將誘捕系統程式事先安裝於各節點，依據管理者搜集的情報，定期依照預設的固定順序的更換節點，透過活動代理人 (mobile agent) 的啓動及關閉系統內的權符 (token)，機動化的部署活動式的誘捕系統，以期大幅降低誘捕系統被反偵測的機會，以對抗駭客日新月異的攻擊手法。倘若發現伺服器已被偵測，則須將此節點列爲黑名單 (blacklist)，不再安裝與部署，避免被駭客群起攻擊，其示意圖如圖 5。

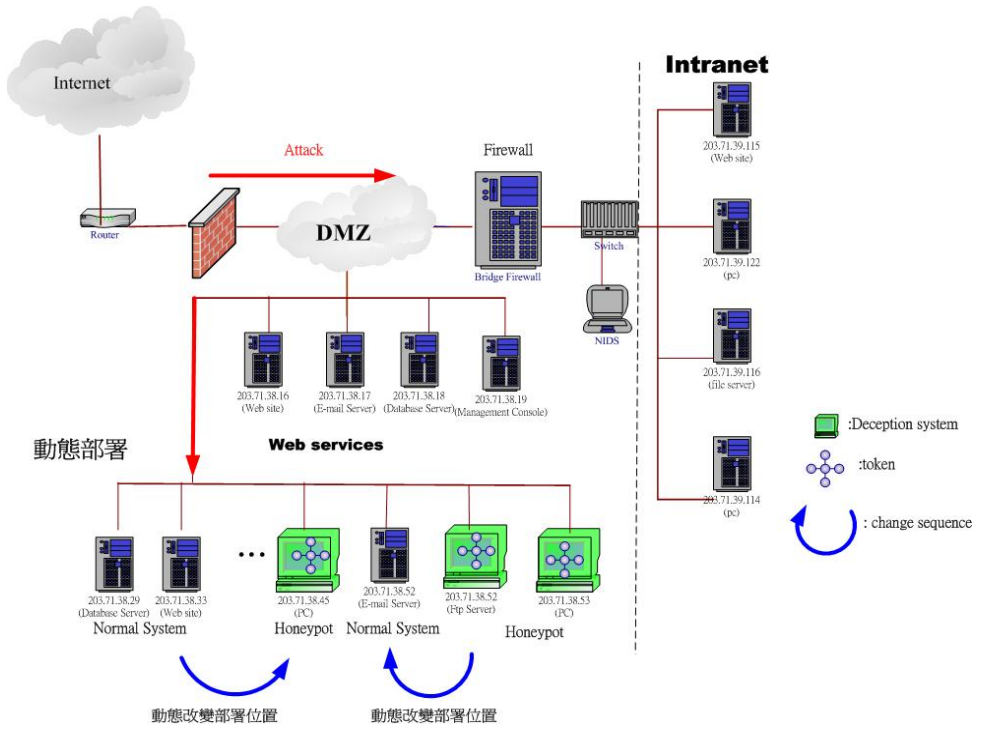

圖 5 機動部署策略

當誘捕系統被活動代理人的啓動權符，則執行誘捕系統的服務；當誘捕系統被活動代理人關閉時，須將此服務留下的指紋資訊（fingerprint）清除，防止被駭客發現。

本研究將誘捕系統預設的位置變化順序設定爲(1)循環式 (round robin)，(2)雜湊函數 (hashing function) 等方法；假設 N 台伺服器 $S_i(i=1,\ldots,N)$，S 代表伺服器的集合，其中金鑰 (Key) $(K_i=1,\ldots,k)$，定義 $P_k(S)$代表一組有序伺服器的子集合，其基數 (cardinality) 爲 k。故在 N 個伺服器，誘捕系統被啓動的可能性 (possibility) N_p 爲

$$N_p = \binom{k}{N} \tag{12}$$

接下來，將每一誘捕系統運作時間定爲 T_i，則在此段時間內，誘捕系統運作的集合(金鑰被啓動的伺服器)爲 $P_k(r)$，其中 r 爲一亂數，例如有 16 台伺服器 (N=16, 主機編號 0~15) 內部裝有誘捕系統，管理者將誘捕系統運作時間定爲 1 小時 (T_i=1)，並機動更改部署位置，若取 r 爲介於 [a, b]區間的亂數，或固定改變的數字或由雜湊函數計算求得，數字的改變可採用下列兩種方法：

(1) 循環式

循環式：例如循環公式取$(2r+1)$，取 r 介於[0,7] 的數字，當 r=0,1,2,…,7 則編號 1，3，5，7，9，11，13，15 伺服器被啓動成爲誘捕系統，8 小時 (r=0~7) 循環一次。此外亦可採用加權輪循 (Weighted Round-Robin)，根據網段主機的重要等級, 給與誘捕系統分配不同的權重，適當的增加誘捕系統的數量或執行時間，提高嚇阻效果。

(2) 雜湊函數

雜湊函數 (hashing function)：雜湊函數將一個數列映射 (mapping) 至[0, N-1]區間，例如取一簡單多項式雜湊函數 $h=15 mod(2r+1)$ 台，當 r=0~100，編號 0，1，2，4，6，15 伺服器隨機的被啓動成爲誘捕系統。系統模擬須考慮不同網路拓樸，例如在 C 級的子網路 (class C subnet) 或平衡樹 (B-tree)，使用上述二種位置變動的策略，誘捕系統位置的預定排程可以由管理伺服器中加以動態排定與變動管理。

4. 實例說明與驗證

以下說明誘捕系統部署節點分析的測試規劃如下:本研究參考 Google 地圖 (Google, 2008)，模擬美國電子商務公司的網路應用服務 (web services)，其主要服務據點設立於美國本土各州的網路節點，規劃實驗網路的拓樸，如圖 6。首先，網路拓樸表示爲一有向圖 $G=(V,E)$，其中網路的頂點集合 (頂點在網路術語爲節點，故以下均採用節點描述)爲 $V=\{v_1, v_2,\ldots, v_n\}$，$E$ 爲圖形的邊 (edge)，公司的服務據點以網路頂點 (vertices) 還表示，兩頂點間連接成邊。

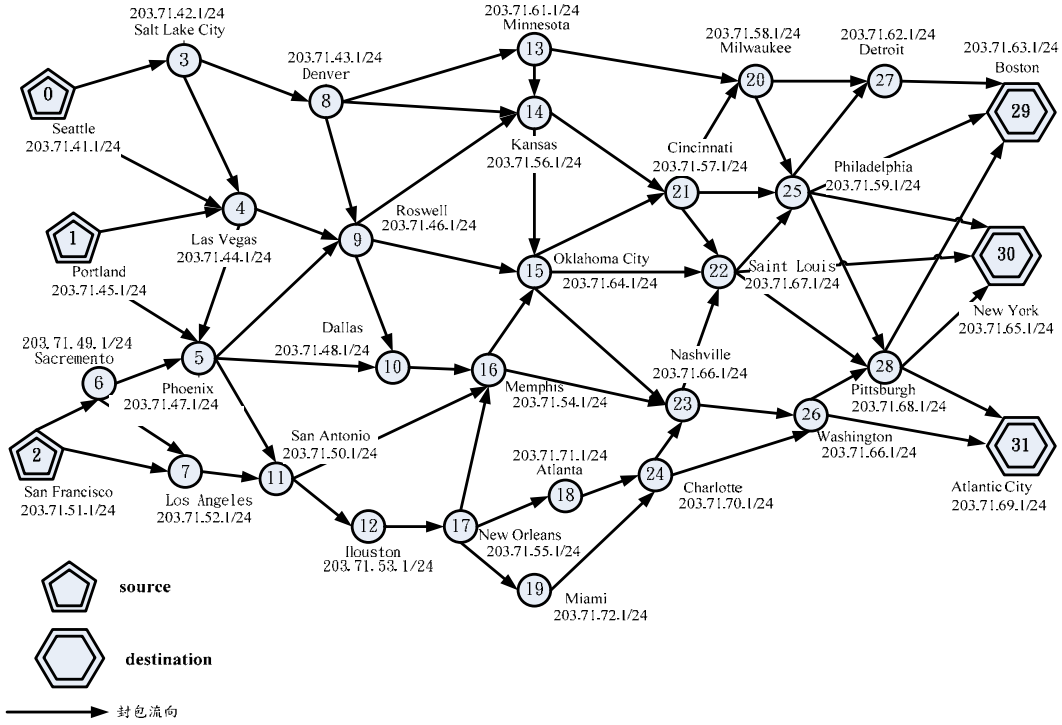

圖 6　美國各城市公司網路實體圖

4.1 部署策略的模擬

本研究將以上述案例執行下列四種部署策略的模擬，首先說明測試程序如下：

(1) 隨機部署策略：

首先經由上述循環式或雜湊函數的公式選出部署的節點，分別取總節點數的 1/2 及 1/4 個節點作爲「預設節點」，因 32 個節點的子網路中共有三個源節點及三個匯節點，故運算總節點數以 26 個節點計算，選出的節點如表 3。在隨機部署策略部份分爲兩個測試案例作分析，分別在

表 3　預設節點表

預設節點	方法	26 個 node 取 1/2 爲 Honeypot	26 個 node 取 1/4 爲 Honeypot
	循環方式	N_4、N_6、N_8、N_{10}、N_{12}、N_{14}、N_{16}、N_{18}、N_{20}、N_{22}、N_{24}、N_{26}、N_{28}	N_4、N_8、N_{12}、N_{16}、N_{20}、N_{24}、N_{28}
	雜湊方式	N_3、N_4、N_5、N_6、N_7、N_9、N_{10}、N_{11}、N_{13}、N_{15}	N_3、N_7、N_{10}、N_{11}、N_{15}

26 個節點中以 1/2 節點及 1/4 作爲隨機部署節點，接下來分別以亂數抽樣的方式取出 13 個節點及 7 個節點，設定爲預設節點如表 4 的第 3 欄，再以蒙地卡羅模擬法（Monte Carlo Simulation）分別對兩測試案例的節點做 500 次隨機部署模擬分析，預測駭客落入預設誘捕系統的節點之機率如圖 6。

(2) 最低成本部署策略：

根據網路服務品質參數值分別將頻寬、穩定度及壅塞程度細分爲 10 種等級，因網路之服務品質因素隨環境動態改變，本案例考量一段時間內，頻寬、穩定度及壅塞程度爲定數，運用等差級數 (1, 0.9,…,0.1, 0.0) 給定相對應傳輸成本如表 5 至 7，若考量動態改變情況，則須加入時間因素，運用動態規劃技術進一步分析。因爲從三個源節點至三個目的節點共有九條最佳路徑如表 8 第 3 欄，故針對每個在最佳路徑上的預設節點作爲「候選部署節點」，並進行網路傳輸成本的加總；因網路傳輸成本與 QoS 值成反比，故可挑選出 QoS 值大於或等於 2.0 (滿分 3 分) 的

表 4 隨機部署節點表

情境	策略	預設節點
隨機部署	26 個 node 取 1/2 爲 Honeypot	N_6、N_7、N_9、N_{12}、N_{14}、N_{15}、N_{16}、N_{19}、N_{20}、N_{21}、N_{25}、N_{27}、N_{28}
		N_4、N_5、N_6、N_7、N_8、N_{10}、N_{13}、N_{18}、N_{19}、N_{20}、N_{22}、N_{24}、N_{26}、N_{28}
		N_5、N_6、N_8、N_{11}、N_{12}、N_{13}、N_{14}、N_{16}、N_{18}、N_{20}、N_{22}、N_{25}、N_{26}
		N_3、N_7、N_8、N_9、N_{11}、N_{12}、N_{13}、N_{15}、N_{19}、N_{20}、N_{21}、N_{26}
	26 個 node 取 1/4 爲 Honeypot	N_4、N_5、N_{13}、N_{15}、N_{19}、N_{22}、N_{26}
		N_5、N_6、N_{12}、N_{14}、N_{15}、N_{21}、N_{26}
		N_6、N_8、N_9、N_{10}、N_{15}、N_{21}、N_{28}
		N_4、N_9、N_{10}、N_{11}、N_{14}、N_{19}、N_{28}

表 5 頻寬成本對照表

等級	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
頻寬	0~	51~	101~	151~	201~	251~	301~	351~	401~	451~
(Mb)	50	100	150	200	250	300	350	400	450	500
成本	1	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1

表 6 穩定度成本對照表

等級	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
穩定度	0.990	0.991	0.992	0.993	0.994	0.995	0.996	0.997	0.998	0.999
成本	1	0.9	0.8	0.7	0.6	0.5	0.4	0.3	0.2	0.1

表 7 壅塞等級成本對照表

等級	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Queue(kb)	1~2	3~4	5~6	7~8	9~10	11~12	13~14	15~16	17~18	19~20
成本	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1

表 8 最佳路徑選擇表

來源端	目的端	最佳路徑
N_0	N_{29}	$N_0 \rightarrow N_3 \rightarrow N_8 \rightarrow N_{13} \rightarrow N_{20} \rightarrow N_{27} \rightarrow N_{29}$
	N_{30}	$N_0 \rightarrow N_3 \rightarrow N_8 \rightarrow N_{13} \rightarrow N_{20} \rightarrow N_{25} \rightarrow N_{30}$
	N_{31}	$N_0 \rightarrow N_4 \rightarrow N_9 \rightarrow N_{10} \rightarrow N_{16} \rightarrow N_{23} \rightarrow N_{26} \rightarrow N_{31}$
N_1	N_{29}	$N_1 \rightarrow N_5 \rightarrow N_{10} \rightarrow N_{16} \rightarrow N_{23} \rightarrow N_{22} \rightarrow N_{25} \rightarrow N_{29}$
	N_{30}	$N_1 \rightarrow N_5 \rightarrow N_{10} \rightarrow N_{16} \rightarrow N_{23} \rightarrow N_{22} \rightarrow N_{25} \rightarrow N_{30}$
	N_{31}	$N_1 \rightarrow N_5 \rightarrow N_{10} \rightarrow N_{16} \rightarrow N_{23} \rightarrow N_{26} \rightarrow N_{31}$
N_2	N_{29}	$N_2 \rightarrow N_6 \rightarrow N_5 \rightarrow N_{10} \rightarrow N_{16} \rightarrow N_{23} \rightarrow N_{22} \rightarrow N_{25} \rightarrow N_{29}$
	N_{30}	$N_2 \rightarrow N_6 \rightarrow N_5 \rightarrow N_{10} \rightarrow N_{16} \rightarrow N_{23} \rightarrow N_{22} \rightarrow N_{25} \rightarrow N_{30}$
	N_{31}	$N_2 \rightarrow N_6 \rightarrow N_5 \rightarrow N_{10} \rightarrow N_{16} \rightarrow N_{23} \rightarrow N_{26} \rightarrow N_{31}$

候選節點作爲「建議部署節點」，其中最大 QoS 值者則選爲「最佳部署節點」，若兩節點的 QoS 值相同，須再比較最低成本路徑經過的次數，挑選經過次數較大者爲「最佳部署節點」。

(3) 已知駭客擁有部份誘捕系統資訊下的部署策略：

此案例運用最低成本部署策略之候選節點，並假設駭客已知部份的節點爲誘捕系統。故首先挑選案最低成本部署策略之候選點中 QoS 值前兩大的節點，作爲駭客已知的節點。因爲駭客最可能經過，但亦較可能被駭客發現，因此誘捕系統部署時，須避開這兩的節點間的最佳路徑，重新規劃部署節點如下：首先，運用與最低成本部署策略相同的測試步驟，分別可找到「建議部署節點」及「最佳部署節點」，接下來，將已知節點擴增爲四個，分析其對部署節點的影響。

(4) 機動部署策略：

首先定義節點編號，因總節點數爲 32，扣除三個源節點及三個匯節點，測試節點總數（N）

爲 26，節點編號令爲 0~25，誘捕系統的動態位置變化順序設定爲奇偶交差，多項式雜湊公式選爲

$$f_d(t) = (2r+t) mod (N-1)，\quad (20)$$

其中 r 爲 0~12 的區間循序漸增變數，t 爲一時間變數，等於 0、1、2、3…。當 r=0,1,…,12 及 t=0 及 1 時，分別啓動偶數 (0,2,4,…,24) 及奇數 (1,3,5,…,25) 節點作爲部署節點，對應的公式分別以 $2r$ 及 $2r$+1。當 t=2 則循環公式改爲以 $2r$+2，部署節點爲 t=0 時的偶數點並加入節點 1，意即節點集合爲 (1,2,4,…,24) 接下來，當 t=4 加入節點 3，達到奇偶交差的目的；當 t=3 則循環公式改爲以 $2r$+3，其部署節點爲 t=1 時的奇數點並加入節點 2，意即節點集合爲 (2,3,5,…,25)。

若考量各啓動節點之網路服務品質，因網路服務品質影響網路封包繞送路徑的重要因素，依各時間點的變化 (t=0,1,2,…)，啓動預設的節點，重新篩選程序，分別選出 QoS 值大於或等於 2.0 者，作爲「建議部署節點」，提高截取駭客攻擊路徑的機率。

以下說明測試結果:

(1) 隨機部署策略：:

預測駭客落入預設節點的機率如圖 7，其中 N_{10} 及 N_{22} 的機率較其他節點高，而 N_7 及 N_{23} 相對於其他節點的機率較低，故運用蒙地卡羅模擬法搭配 NS2 工具，可分析落入誘捕次數相對較高的節點，作爲部署誘捕系統的「建議部署節點」，可增加誘捕機率。

(2) 最低成本部署策略：

經由公式規劃出部署節點後，由三個來源端發送訊息至三個匯端，依據最低成本原則，選出兩端間的九條最佳路徑，接下來，針對每個節點，在最佳路徑上的預設節點進行網路成本的加總，因網路傳輸成本與 QoS 值成反比，再由後選節點中挑選出 QoS 值大於、等於 2.0 者 (滿

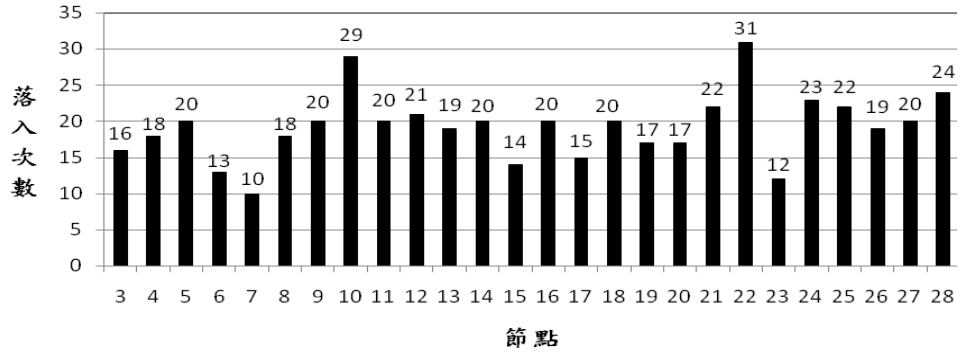

圖 7 駭客落入預設誘捕系統節點的機率

分 3 分) 爲建議部署節點，其結果爲 N_3、N_6、N_{20} 及 N_{26}，如表 9 第 3 欄；選擇最大 QoS 值爲最佳部署節點，其結果爲 N_3、N_6 及 N_{20}，如表 9 第 4 欄。

(3) 已知駭客擁有部份誘捕系統資訊下的部署策略：

考量駭客擁有部份資訊的情況下，假設駭客已知二個及四個高流量節點的情況下，以網路服務品質重新篩選程序，經過計算分析出誘捕系統最佳部署節點分別爲 N_5、N_6、N_9、N_{11}、N_{15} 及 N_{28}，計算結果如表 10 第 4 欄。

(4) 機動部署策略：

由上述公式分別計算出 t_0 及 t_1 的預設節點後，以隨機取樣的方式取出五個節點作爲啓動節點如表 11 第 4 欄，再考量各啓動節點的網路服務品質，綜整 QoS 大於、等於 2.0 之啓動節點，作爲誘捕系統的「建議部署節點」如表 11 第 5 欄。

4.2 四種策略的比較分析

透過上述四個佈署策略模擬，可分析出各個不同策略的建議部署節點或最佳部署節點，其中後三個策略挑選部署節點方式，皆以網路傳輸成本做考量，若在網路各節點的網路傳輸成本皆固定的情況下，策略一隨機選取是以蒙地卡羅模擬法作挑選預設節點的公式，當測試次數越少時，因產生亂數不均勻，各預設節點攔截駭客的命中機率較不均等，但隨模擬次數增多，則各節點命中機率則趨近於平均，假設駭客利用隨機單點攻擊，則誘捕機率爲部署誘捕系統數量/網路節點數。

而策略二的最低成本部署策略未考慮動態改變位置，故最佳部署節點隨網路 QoS 數值變化，當發生壅塞或斷線，最佳部署節點會產生改變。假設 1/2 網路節點選爲誘捕系統，網路設備以表 8 的最佳路徑來選擇爲繞送路徑，以表 9 的案例一爲例，部署誘捕系統數量可由 13 個節點降至 3 個建議部署節點 (N_6,N_{20},N_{26})，因爲 3 個建議部署節點涵蓋九條最佳路徑中的八條，故誘捕機率可由策略一的 0.5 提高至 0.89 (8/9)。

策略三在假設駭客知道某些節點爲誘捕系統後，其行經的最佳路徑將改變，故誘捕系統的最佳部署節點將避開特定節點，建議部署節點與策略二的結果有所不同。策略四以模擬機動部署方式，事先完成誘捕系統的安裝，在不同時間點啓動預設的誘捕系統，定時動態改變部署位置，使駭客不易查覺誘捕系統，可大幅提高誘捕系統的安全性；若策略四同時考量網路服務品質因素，先挑選出流量大且連線狀況好的部署節點，如此同時兼顧部署的有效性及安全性，四種策略比較如表 12。

表 9 最低成本部署策略之建議節點選擇表

欄位編號	1	2	3	4
情境	方法	候選節點 (QoS 值)	建議部署節點	最佳部署節點
最低成本部署	循環方式（26 個 node 取 1/2 爲 Honeypot）	N_4（1.5）、N_6（2.0）N_8（1.8）、N_{10}（1.8）N_{16}（1.5）、N_{20}（2.2）N_{22}（1.2）、N_{26}（2.1）	N_6、N_{20} N_{26}	N_{20}
	循環方式（26 個 node 取 1/4 爲 Honeypot）	N_4（1.5）、N_8（1.8）N_{16}（1.5）、N_{20}（2.2）	N_{20}	N_{20}
	雜湊函數（26 個 node 取 1/2 爲 Honeypot）	N_3（2.0）、N_4（1.5）N_5（1.9）、N_6（2.0）N_9（1.6）、N_{10}（1.8）N_{13}（1.9）	N_3、N_6	N_6
	雜湊函數（26 個 node 取 1/4 爲 Honeypot）	N_3（2.0）、N_{10}（1.8）	N_3	N_3

表 10 駭客已知部份節點爲誘捕系統時建議部署選擇表

欄位編號	1	2	3	4
情境	策略	攻擊者已知節點	建議部署節點 QoS	最佳部署節點
駭客已知部份節點爲誘捕系統時	循環方式 (26 個 node 取 1/2 爲 Honeypot)	N_{20}、N_{26}	N_4（1.5）、N_{16}（1.5）N_{22}（1.2）、N_{28}（2.1）	N_{28}
		N_{16}、N_{20} N_{26}、N_{28}	N_4(1.5)、N_6(2.0)N_8(1.8)、N_{22}（1.2）	N_6
	循環方式 (26 個 node 取 1/4 爲 Honeypot)	N_8、N_{20} N_4、N_8 N_{16}、N_{20}	N_4（1.5）、N_{16}（1.5） 無(預設節點無流量經過)	N_{16} 無
	雜湊函數 (26 個 node 取 1/2 爲 Honeypot)	N_3、N_6	N_4(1.5)、N_5(1.9)N_7(1.7)、N_9(1.6)N_{11}(1.9)、N_{15}(1.4)	N_5
		N_3、N_5 N_6、N_{11}	N_4(1.5)、N_9(1.6)N15(1.4)	N_9
	雜湊函數 (26 個 node 取 1/4 爲 Honeypot)	N_3、N_{10} N_3、N_7 N_{10}、N_{11}	N_7(1.7)、N_{11}(1.9)N_{15}(1.4) N_{15}（1.4）	N_{11} N_{15}

表 11 動態部署節點選擇表

欄位編號	1	2	3	4	5
情境	位置變化公式	時間	預設節點	啓動節點	建議部署節點 (QoS>=2.0)
動態部署	$f_d(t) = (2r+t) mod (N-1)$	t_0	N_3、N_5、N_7、N_9	N_3	N_{13}
			N_{11}、N_{13}、N_{15}	N_5	
			N_{17}、N_{19}、N_{21}	N_{13}	
			N_{23}、N_{25}、N_{27}	N_{21}	
				N_{27}	
		t_1	N_4、N_6、N_8、N_{10}	N_8	N_{18}
			N_{12}、N_{14}、N_{16}	N_{14}	N_{26}
			N_{18}、N_{20}、N_{22}	N_{18}	
			N_{24}、N_{26}、N_{28}	N_{22}	
				N_{26}	

表 12 部署策略的決策選擇

	決策因素	效用
策略一	未蒐集網路路徑數據與 QoS 資訊，則可採用隨機部署策略	網路節點爲 n，隨部署誘捕系統數量 k 增加而上昇，假設駭客利用隨機單點攻擊，誘捕機率爲 k/n，但部署數量增加將增加維護成本
策略二	若蒐集網路路徑數據與 QoS 資訊，可選擇「最低成本部署策略」，但當網路連線發生壅塞或斷線，最佳部署節點會改變	與策略一比較，由表 8 及表 9 的案例一得知，部署誘捕系統數量可由 13 個節點降至 3 個建議部署節點，節省 77%經費，而誘捕機率可由策略一的 0.5 提高至 0.89
策略三	已知駭客掌握部份誘捕系統資訊下，則須採用此策略	避開駭客已知節點，計算誘捕機率與最低成本部署策略相似
策略四	可結合最低成本部署策略，動態改變部署位置，使駭客不易查覺誘捕系統	挑選出流量大且連線狀況好的部署節點，動態更換誘捕系統位置，可提高誘捕系統的部署的有效性及安全性

4.3 方法的比較

本研究以 Cohen (2000) 所提出的網路欺敵的方法做爲比較，其所提出的誘捕系統部署，是運用系統的弱點，透過多址技術，模擬數量龐大的虛擬誘捕系統，增加誘捕的機率，但其採用隨機部署策略，未考量繞送路徑最佳化，缺乏進一步規劃性。而本研究運用動態部署策略做爲基礎，考量網路服務品質，透過最佳路徑分析，推估出最低網路傳輸成本的路徑作爲駭客最可能經過的路線，進而部署誘捕系統以提高誘捕機率。兩方法的特色、限制及適用範圍如表 13。

5. 結論與未來研究方向

本研究參考 Lance (2003) 的新觀念，修改原有佈雷區策略及延伸 Cohen (2000) 的隨機部署方法，發展一套『誘捕系統的動態部署決策模式』，透過最低傳輸成本，找出兩端點間的所有可行路徑，考量網路服務品質因素下，透過隨機部署、最低成本部署、駭客擁有誘捕系統資訊的狀況下及動態部署策略比較分析，進而計算出誘捕系統的最佳部署節點，此決策模式可運用於掌控度高的網路環境下之誘捕系統部署，如企業內部網路或重要設備相鄰的局部網路，但對於廣大的網際網路，則因網路服務品質動態改變，無法即時掌握及作出精確的部署；未來研究方向將朝賽局理論進行駭客與誘捕系統的對抗研究，運用賽局理論的分析，建立網路攻擊的數學模型，模擬駭客不同攻防策略，透過兩人零和賽局 (two person, zero-sum game)，找出誘捕系統的最佳部署策略，驗證所提部署策略及節點選用的限制，作爲誘捕系統部署改進的參考。

表 13　方法的比較

	本研究方法	Cohen (2000)
特色	修改佈雷區部署策略，運用動態部署，並選取最低傳輸成本的路徑中的節點進行部署，可有效降低部署的數量及提高誘捕機率	採用佈雷區部署策略，透過多址技術，模擬出眾多誘捕系統，隨機部署，以虛真相間方式部署，提高誘捕機率
限制	需事先蒐集網路路徑數據與 QoS 資訊	無需事先蒐集網路路徑數據與 QoS 資訊
適用範圍	較適用於掌控度高的內部網路部署的精密部署	較適用於不熟悉網路或開放式網路的部署

參考文獻

王平、蘇浩儀、顏柏璋、王建仁，「誘捕系統動態部署模式的建立與分析」，第十七屆資訊安全會議研討會論文集，嘉義：中華民國資訊安全學會，民國 96 年，661-670 頁。

黃志雄、王智弘，「整合代理人入侵偵測系統與陷阱誘捕系統之研究」，嘉義大學資訊工程系未出版碩士論文，民國 93 年。

賽門鐵克研究實驗室，入侵偵測系統：誘捕式網路防禦技術的演進，民國 94 年，檢索日期：民國 96 年 1 月 16 日，取自 http://www.symantec.com/region/tw/enterprise/article/mantrap.html。

Chen, P. T., Laih, C. S., Pouget, F., and Dacier, M., "Comparative Survey of Local Honeypot Sensors to Assist Network Forensics," unpublished paper presented at First International Workshop on Systematic Approaches to Digital Forensic Engineering, Taipei, Taiwan, Nov 7-9, 2005.

Cohen, F. and Associates, "Deception Toolkit", 1998. Retrieved January 12, 2007, from http://all.net/dtk/dtk.html.

Cohen, F., "A Mathematical Structure of Simple Defensive Network Deception," *Computers and Security*, Vol. 19, No. 6, 2000, pp. 520-528.

Dornseif, M., Holz, T., and Klein, C. N., "Nose Break-attacking Honeynets," In *Proceedings of 5th Annual IEEE Systems, Man and Cybernetics Information Assurance Workshop*, West Point, New York: IEEE Computer Society Press, 2004, pp. 123-129.

Gupta, N., "Improving the Effectiveness of Deceptive Honeynets through an Empirical Learning Approach," unpublished paper presented at the Australian Information Warfare and Security Conference, Perth, Western Australia, November 28-29, 2002.

Google Inc., "Google Maps." Retrieved January 10, 2007, from http://maps.google.com/

Hernacki B., Bennett J., and Lofgren, T., "Symantec Deception Server Experience with a Commercial Deception System," *Lecture Notes in Computer Science*, Vol. 3224, 2004, pp. 188-202.

Honeynet Project, "Know Your Enemy: Statistics, Analyzing the Past and Predicting the Future," 2001. Retrieved March 6, 2007, from http://www.honeynet.org/papers/stats/.

Keong, T. C., "Detecting Sebek Win32 Client", 2004. Retrieved March 8, 2007, from http://www.security.org.sg/vuln/ sebek215.html.

Lance, S., "Dynamic Honeypots," 2003a. Retrieved March 8, 2007, from http://www.securityfocus.com/infocus/1731.

Lance, S., "Honeypot Farm," 2003b. Retrieved March 8, 2007, from http://www.securityfocus.com/infocus/1720.

McMullen, J. F., “Enhance Intrusion Detection with a Honeypot,” 2004. Retrieved March 12, 2007, from http://articles.techrepublic.com.com/5100-1035_11-1042983.html

Pelletier, B., “Connection Redirection Applied to Production Honeypots,” 2004. Retrieved March 12, 2007, from http://www.eruditeaegis.net/papers/redirection_honeypot.pdf.

Skvarcius, R. and Robinson, W. B., *Discrete Mathematics with Computer Science Applications,* Menlo Park, CA: Benjamin, Cummings, 1986.

Sherif, M. K., Chatree, S., Daniel, M., Rami, M., and Taieb, Z., “Roaming Honeypots for Mitigating Service-level Denial-of- Service Attacks,” In *Proceedings of the 24th International Conference on Distributed Computing Systems*, Hachioji, Tokyo: IEEE Computer Society Press, 2004, pp.328-337.

Valli, C., “Honeypot Technologies and Their Applicability as an Internal Countermeasure,” unpublished paper presented at the 3rd Australian Computer, Information and Network Forensics Conference, School of Computer and Information Science, Edith Cowan University, Mount Lawley, Western Australia, September 29, 2005.