誘捕系統欺敵與部署策略的研析

王 平，蘇浩儀
Wang Ping, Su Hao-Yi
資訊管理系 資訊科技學院 崑山科技大學
E-mail:pingwang@mail.ksu.edu.tw

摘要

近年來資安組織執行誘捕系統(honeypot)部署時，時常發現資訊蒐集效果不彰，即使部署完成，卻無法吸引攻擊者前來探測，故如何選擇部署節點及降低被反偵測的機率是誘捕系統部署的重要議題。本研究結合機率與網路路徑分析技術論，建立一個誘捕系統的部署分析數學模式，改進現有靜態佈雷區及網路欺敵為主的部署策略，採用動態部署策略，估算誘捕機率；此外，本研究將假設在不同的網路服務品質(QoS)環境下，運用最小成本法以分析駭客連線的最佳路徑，進而選擇的最佳部署節點。系統驗證將以 NS2(Network Simulator, version2)工具模擬隨機部署及動態部署策略，比較及分析案例中的網路「建議部署節點」與「最佳部署節點」。
關鍵字：誘捕系統、佈雷區、動態部署、隨機部署、最佳部署節點

1. 前言

隨著網路技術演進，資安組織成功運用入侵偵測系統 (Intrusion Detection System; IDS)，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為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(honeypot) 是指單一主機，誘捕網路系統(Honeynet)則是一個網路系統，這一網路系統是隱藏在防火牆後面，所有進出的資料都可能受到監控、捕獲及控制。此外，現行的 Honeynet 防護策略是在每一服務伺服器均對應一個誘捕系統，可將進出伺服器的異常通訊連線，指向對應的誘捕系統主機來處理。這種將可疑連線作轉移的方法，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。基於上述理由，本研究發展一個『誘捕系統部署策略分析模式』，其目的為發展一個不須轉移連線的動態部署策略，達到「網路欺敵」；此外，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作業品質。

2. 文獻探討

Cohen（2000）研析以網路拓樸(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，運用多址(multi-home) 技術以一個主機模擬64,000個誘捕系統，散佈於眾多真實系統間，以提高誘捕機率。

Lance (2003) 提出兩個誘捕系統佈署的新觀念:「機動誘捕系統(dynamic honeypot)」與「誘捕系統莊園(honeypot farms)」。「機動誘捕系統」為一隨插即用(plug-and-play)部署方法，藉由自動化計算部署數量，如何部署及如何偽裝與現有環境相契合，降低被反偵測的可能性。「誘捕系統莊園」的觀念是捨棄大量部署的策略，透過部署簡易的偵測器(類似哨兵)，若發現可疑連線，則轉移至堅固防護的誘捕系統莊園。

Sherif, et al. (2004)提出活動式的誘捕系統(roaming honeypot)部署方式，以對抗分散式阻斷服務(DDOS)攻擊，上述的研究採用隨機部署，沒有針對現有的佈雷區、防護罩及活動式部署策略，以理論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為何。

3. 誘捕系統部署策略與分析

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，故資訊偽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，首要考慮「降低被反偵測的機率」及「部署的有效性」兩項需求。

3.1.1 佈雷區的部署策略

佈雷區(Minefield)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。誘捕系統 常部署在 DMZ 區域中的外部伺服器之間，捕捉針對網路服務伺服器及內部網路的攻擊。早期誘捕系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(Deception Toolkit, DTK)被研發出來，以解決上述問題。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 IP/port 位址空間，(2) 運用大量的 IP/port 位址部署，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。此外，他提出以下兩個改善 DTK 的偵測能力的解決方法，以「偽裝」誘捕系統，降低被駭客偵測的機率:

(1)一址多戶(multi-home in a box) (2) 多址解決方案(multiple addresses resolution)，透過多址解決方案技術，最高可達 64,000 IP 位置被模擬作為虛擬的誘捕系統，並將此命名為 D-WALL。D-WALL 與 DTK 的不同點是: DTK 是增加部署誘捕裝置於 IP/port 位址空間；而 D-WALL 除了增加更多的誘捕裝置部署於 IP/port 位址空間外，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的興趣，佈雷區的部署策略示意圖如圖 1。

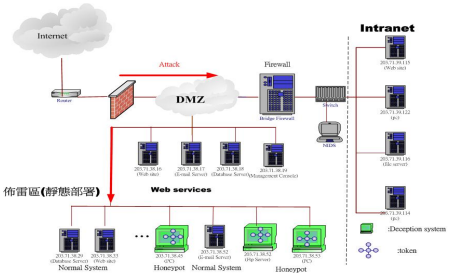

圖 1 佈雷區的誘捕系統的部署策略

案例 I：最低成本部署策略

因篇幅局限，最低成本部署數學模式的建立，請參考先前研究－王 平，蘇浩儀等(民 96)之第十七屆資訊安全會議研討會(ISC2007)發表的「誘捕系統動態部署模式的建立與分析」，第四頁。

案例 II：隨機部署策略

舉例來說，如果在某個網段(network subnet)中，在 200 台伺服器部署 50 個誘捕系統，理論上，駭客利用隨機單點攻擊，則駭客落入誘捕系統的機率是 20%，其運算公式為:

$$P_h = N_h / (N_r + N_h) \qquad (1)$$

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

案例 III：動態部署策略

在選擇誘捕系統部署是固定的網址，駭客終將以探測工具找到部署的位置。故本研究提出動態部署(dynamic deployment)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)的啟動(enable)及關閉系統內的權符(token)，機動化的部署活動式的誘捕系統(roaming honeypot) (Sherif, et al., 2004)，可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，則須將此節點列為黑名單(blacklist)，避開此節點部署，避免被駭客群起攻擊，其示意圖如圖 2。

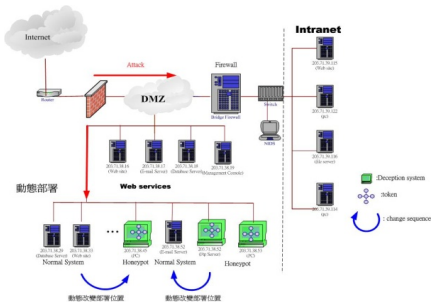

圖 2 動態式誘捕系統的部署策略

當誘捕系統被活動代理人的啟動(enable)權符時，本系統將採用權符(token)控制，須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（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為(1)循環式如round robin方式 (2)雜湊函數(hashing function)的選定等策略；假設伺服器(S_i)，S代表有N個伺服器的集合或子集合(i=1,…,N)，其中金鑰(Key) (K_i=1,…,k)，定義P_k(S)代表一組有序可能的子集合，其基數(cardinality)為k。故在N個伺服器，誘捕系統被啟動的可能性(possibility) N_p為

$$N_p = \begin{pmatrix} k \\ N \end{pmatrix} \qquad (2)$$

接下來，將每一誘捕系統運作時間定為T_i，則在此段時間內，誘捕系統運作的集合(金鑰被啟動的伺服器)為 $P_k(r)$，其中r為一亂數(random)，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為 1 小時(T_i=1)，並機動更改部署位置，若取r 為介於[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。可採用下列兩種方法:

CASE I: 循環式

循環式：如輪循(round robin)方式，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 伺服器被啟動成為誘捕系統，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, 給予誘捕系統不同的權重，適當的增加誘捕系統的數量或執行時間，提高嚇阻效果。

CASE II: 雜湊函數

雜湊函數(hashing function) 方式：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=15mod(2r+1)台，當 r=0~100，編號 0，1，2，4，6，15 伺服器隨機的被啟動成為誘捕系統。

系統模擬考慮不同網路拓樸，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. 模式的模擬與驗證

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各州的網路節點，規劃實驗網路的拓樸(Topology)，如圖 3。首先，網路拓樸表示為一有向圖G=(V,E)，其中網路的頂點(vertices)集合(頂點在圖形理論術語，對應的網路用語為節點，故以下均採用節點描述)，V={v_1, v_2,..., v_n}，E為圖形的邊(edge)，公司的服務據點以網路節點表示，兩頂點間連接成邊。

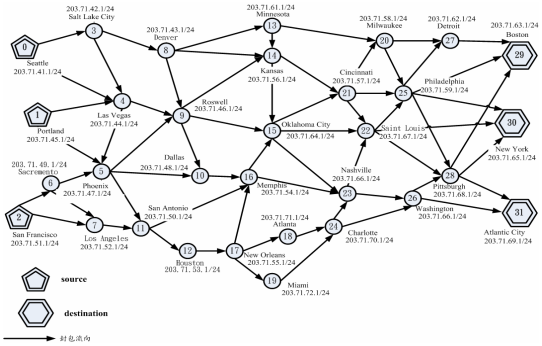

圖 3 美國各城市公司網路實體圖

4.1 模式的模擬

本研究將以上述案例做下列三種狀況的模擬實驗:

(1) 最低成本部署策略：

首先經由上述 CASE I 與 CASE II 的公式規劃出預設部署的節點，分別取總節點數的 1/2 及 1/4 個節點作為「預設節點」，因 32 個節點中分別有三個來源端及三個目的端，故運算總節點數以 26 個節點計算。接著根據網路服務品質參數值分別將頻寬、穩定度及壅塞細分為 10 種等級，再運用等差級數(1、0.9、0.8…0)給予相對應傳輸成本（因篇幅局限相關成本表格請參王 平，蘇浩儀等(民 96)之第

十七屆資訊安全會議研討會(ISC2007)發表的「誘捕系統動態部署模式的建立與分析」)。因為從三個源節點至三個目的節點共有九條最佳路徑如表 1 第 3 欄，故針對每個在最佳路徑上的預設節點進行網路成本的加總作為「候選部署節點」，再挑選出 QoS 值大於、等於 2.0(滿分 3 分)的候選節點作為「建議部署節點」。「最佳部署節點」則選擇最大 QoS 值者，若兩節點的 QoS 值相同，則再比較最佳路徑經過的次數，挑選次數較多者為「最佳部署節點」。

(2) **隨機部署策略:**

在隨機部署策略部份，首先在 26 個節點中選出 1/2 及 1/4 節點作為隨機部署節點，接下來，分別以亂數取樣的方式取出 13 個節點及 7 個節點，設定為預設節點如表 3 第 3 欄，再以蒙地卡羅模擬法（Monte Carlo Simulation）分別對兩案例的節點做 500 次隨機部署，並分析出駭客落入規劃誘捕系統的節點之命中機率如圖 4。

(3) **動態部署策略**：

根據上述的動態部署策略說明，首先定義節點編號，因總節點數為 32，測試節點總數（N）為 26 (因 32 個節點扣除三個來源端及三個目的端節點)，節點編號令為 0~25 (0,1,..,N-1)，誘捕系統的動態位置變化順序設定為奇偶交差方式，公式可表示為

$$f_d(t) = (2r+t)\bmod(N-1) \qquad (3)$$

其中 r 為 0~12 的區間循序漸增變數，t 為一時間變數，等於 0、1、2、3…。當 r=0,1,…,12 及 t=0 及 1 時，分別啟動偶數(0,2,4,…,24)及奇數(1,3,5,…,25)節點作為「啟動節點」，對應的公式分別以 2r 及 2r+1。當 t=2 則循環公式改為以 2r+2，啟動節點為 t=0 時的偶數點並加入節點 1，意即節點集合為 (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 則循環公式改為以 2r+3，其啟動節點為 t=1 時的奇數點並加入節點 2，意即節點集合為(2,3,5,…,25)。

因 QoS 乃影響網路封包繞送路徑的重要因素，故須考量各啟動節點之網路服務品質(QoS)，依各時間點的變化(t=0,1,2,…)，啟動預設的節點，以 QoS 重新篩選程序，篩選程序同最低成本部署策略，分別選出 QoS 大於、等於 2.0 者，作為「建議部署節點」，提高截取駭客攻擊路徑的機率。

案例測試

案例 1 最低成本部署策略：

經由公式規劃出部署節點後，依據最低成本原則，綜整出建議部署節點為 N3、N6、N20 及 N26，如表 2 第 4 欄；選擇最大 QoS 值為最佳部署節點，其結果為 N3、N6 及 N20，如表 2 第 5 欄。

案例 2 隨機部署策略:

經由綜整出駭客落入預設節點的相對次數如圖 4，分析出 N10 及 N22 落入次數較其他節點高，而 N7 及 N23 落入次數較其他節點低，故蒙地卡羅模擬法可分析出出現次數較高的節點，作為部署誘捕系統的「建議部署節點」，可增加誘捕機率。

案例 3 動態部署策略:

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為啟動節點如表 4 第 4 欄，再考量各啟動節點的 QoS 值，綜整出 QoS 大於、等於 2.0 之啟動節點作為誘捕系統的建議部署節點如表 4 第 5 欄。

表 1 最佳路徑選擇表

來源端	目的端	最佳路徑	傳輸成本
N0	N29	N0→N3→N8→N13→N20→N27→N29	9.6
	N30	N0→N3→N8→N13→N20→N25→N30	9.5
	N31	N0→N4→N9→N10→N16→N23→N26→N31	9.9
N1	N29	N1→N5→N10→N16→N23→N22→N25→N29	9.4
	N30	N1→N5→N10→N16→N23→N22→N25→N30	9.4
	N31	N1→N5→N10→N16→N23→N26→N31	8.7
N2	N29	N2→N6→N5→N10→N16→N23→N22→N25→N29	11.4
	N30	N2→N6→N5→N10→N16→N23→N22→N25→N30	11.4
	N31	N2→N6→N5→N10→N16→N23→N26→N31	10.7

表 2 最低成本建議節點選擇表

情境	策略	候選部署節點 (QoS 值)	建議部署節點	最佳部署節點

最低成本部署	循環部署（26 個 node 取 1/2 為 Honeypot）	N4（1.5）、N6（2.0） N8（1.8）、N10（1.8） N16(1.5)、N20(2.2)、 N22（1.2）N26（2.1）	N6 N20 N26	N20
	循環部署（26 個 node 取 1/4 為 Honeypot）	N4（1.5）、N8（1.8） N16（1.5）、N20（2.2）	N20	N20
	雜湊部署（26 個 node 取 1/2 為 Honeypot）	N3（2.0）、N4（1.5） N5（1.9）、N6（2.0） N9（1.6）、N10（1.8） N13（1.9）	N3 N6	N6
	雜湊部署（26 個 node 取 1/4 為 Honeypot）	N3（2.0）、N10（1.8）	N3	N3

表 3 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 為 Honeypot	N6、N7、N9、N12、N14 N15、N16、N19、N20 N21、N25、N27、N28
		N4、N5、N6、N7、N8、N10 N13、N18、N19、N20、N22 N24、N26、N28
		N5、N6、N8、N11、N12 N13、N14、N16、N18、N20 N22、N25、N26
	26 個 node 取 1/4 為 Honeypot	N4、N5、N13、N15、N19 N22、N26
		N5、N6、N12、N14、N15 N21、N26
		N6、N8、N9、N10、N15 N21、N28

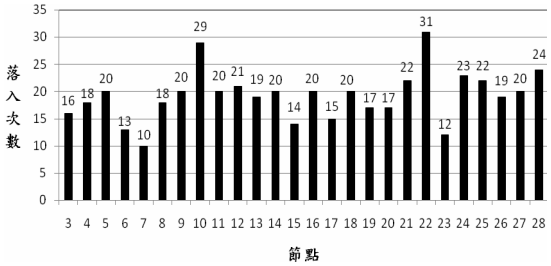

圖 4 駭客落入預設節點的機率圖

表 4 動態部署節點選擇表

情境	時間	預設節點	啟動節點	建議部署節點 (QoS>=2.0)
動態部署	t_0	N3、N5 N7、N9 N11、N13 N15、N17 N19、N21 N23、N25 N27	N3 N5 N13 N21 N27	N3
	t_1	N4、N6 N8、N10 N12、N14 N16、N18 N20、N22 N24、N26 N28	N8 N14 N18 N22 N26	N18 N26

4.2 討論

在上述兩個案例模擬中，案例二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，因亂數產生的不均勻，各預設節點攔截駭客的命中機率較不平均，當測試次數越多則命中機率較趨近於平均。案例三以模擬動態部署方式，在不同時間點啟動預設的誘捕系統，在網路 QoS 的考量下，再挑選出流量大且連線狀況好的部署節點，此作為不但可以節省誘捕系統的部署成本，更可讓駭客不易破解誘捕系統啟動的規則（因動態改變部署位置），提高誘捕率及誘捕系統的有效性。而在盲目部署的情況下其計算誘捕機率公式為 n/m，其中 n 為部署節點，m 為網路總節點數，以本研究案例 26 個節點中部署 3 個誘捕系統，其命中機率為 11.5(3/26)，而選擇最佳路徑上 QoS 之節點作部署誘捕系統，則可提高誘捕率至 70%，高出盲目部署機率達六倍以上。例如選擇 N23 部署節點，則有 7 條最佳路徑通過此點，故若能夠掌握網路上的 QoS 參數，搭配誘捕系統的動態配置，將可提高誘捕機率。

4.3 建議部署點方法的比較

本研究以 Fred Cohen(2000)所提出的”A Mathematical Structure of Simple Defensive Network Deception ”的方法作為比較。Fred Cohen 所提出的誘捕系統部署，是運用系統的弱點，運用 DTK 工具模擬虛擬誘捕系統，主要是運用欺敵的方式，透過大量部署，以量取勝，增加駭客落入誘捕系統的機率，其採用是隨機部署策略，方法簡單不必考慮部署網路的特性。但也因未考量繞送路徑最佳化，部署缺乏進一步規劃，可能降低誘捕機率。而本研究運用動態部署策略作為基礎，並考量到網路服務品質，透過最佳路徑分析，參考 QoS 值的大小，推估出最低網路傳輸成本的路徑(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 5。

表 5 方法的比較

	本研究方法	Fred Cohen
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，可有效提高誘捕機率，增加誘捕系統的存活率	採用佈雷區部署策略，運用 DTK 可模擬出眾多誘捕系統，隨機部署，以虛真相間方式部署
限制	需事先蒐集網路 QoS 資料與數據	勿需事先蒐集網路 QoS 資料與數據

適用範圍	較適用於精密的部署或掌控度高的網段部署	較適用於不熟悉網段或粗略的部署

5. 結論與未來研究方向

本研究修改原有佈雷區策略及延伸 Fred Cohen(2000)的隨機部署方法，發展一套『誘捕系統的部署分析模式』，透過最低成本分析出兩節點間的最佳路徑，再考量網路服務品質因素，同時考量隨機部署及動態部署策略，進而計算出誘捕系統的最佳部署節點；未來研究方向將朝以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，以模擬駭客不同攻防狀況，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，作為誘捕系統部署改進的參考。

誌謝

感謝成功大學資通安全研究與教學中心(TWISC@NCKU)技術支援，部份經費由國家科學委員會計劃編號NSC 96-2219-E-006-009及NSC 95-2219–E-168-001支援。

參考文獻

[1] 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(ISC2007)」，國立嘉義大學，661~670 頁，民國 96 年 6 月 8 日。

[2] 成功大學資通安全及教學中心，http://www.twisc.nctu.edu.tw/。

[3] 賴光威、江至軒，「藉由動態調適 競爭/免競爭比例以強化 IEEE 802.11e 之 QoS 支援」，國立中山大學資訊工程學系研究所未出版碩士論文，民國 93 年。

[4] 賽門鐵克研究實驗室(民 94)，入侵偵測系統：誘捕式網路防禦技術的演進。

[5] Cohen, F., “A Mathematical Structure of Simple Defensive Network Deception” Computers and Security 19/6, 2000, pp.520-528.

[6] Dornseif, M., Holz, T., and Klein, C., “Nose break-attacking honeynets”, in *Proceedings of 5th Annual IEEE Information assurance workshop*, 2004

[7] Gupta, N., “Improving the Effectiveness of Deceptive Honeynets through an Empirical Learning Approach”, School of Computer and Information Science Edith Cowan University, Australia, 2003.

[8] Hernacki B., et al.(2004),"Symantec Deception Server Experience with a Commercial Deception System, " LNCS, Vol.3224.

[9] Hernacki, B. et al., “Symantec Deception Server Experience with a Commercial Deception System,” LNCS, 3224, 2004.

[10] Hillier, S. F. and Lieberman, G. J., *Introduction to Operations Research*, McGraw Hill, New York, 2005.

[11] Lance S. (2003), “Dynamic Honeypots.” http://www.securityfocus.com/infocus/1732

[12] Lance S. (2003), “Honeypot Farm.” http://www.securityfocus.com/infocus/1720

[13] McMullen, J. F., “Enhance intrusion detection with ahoneypot”,2004.http://articles.techrepublic.com.com/5100-1035_11-1042983.html

[14] Pelletier, B. “Connection Redirection Applied to Production Honeypots”, Norwich University, 2004.

[15] Sherif M. Khattab et al. (2004), " Roaming Honeypots for Mitigating Service-level Denial-of-Service Attacks, "Proceedings of the 24th International Conference on Distributed Computing Systems (ICDCS’04)

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

[17] Shuping, R, “A Model for Web Services Discovery With QoS, ”ACM SIGecom Exchanges, 4/1, 2003, pp.1-10.