賽局理論在資訊安全上的應用
—以網路入侵偵測節點的最經濟配置爲例

吳正光
國立中央大學資訊管理學系
中大路300號
桃園縣320中壢市
93443002@cc.ncu.edu.tw

陳奕明
國立中央大學資訊管理學系
中大路300號
桃園縣320中壢市
cym@mgt.ncu.edu.tw

吳大任
國立中央大學經濟學系
中大路300號
桃園縣320中壢市
drwu@mgt.ncu.edu.tw

摘要

如果考量有限的成本，現行的網路入侵偵測系統在攻擊偵測能力與使用者存取網路的容易程度之間存在著權衡的問題，本研究以非合作與合作賽局模型整合成一個架構來配置經濟的網路入侵偵測系統（IDS），第一個模型描述與分析單一攻擊者與入侵偵測節點間的互動關係，並將其對應爲一個非零和、雙人與非合作的賽局，經由計算得到每個偵測節點的混合策略納許均衡作爲安全的風險值，再以這風險值考量在不同的安全警戒程度下，計算每個偵測節點影響其它節點的夏普力值，因此可以在特定的成本下得到一個具有公平性的配置偵測節點集合。本研究用數值案例驗證兩模型，結果顯示：網路管理者可以量化評估偵測節點的安全風險值，並依據各種不同的威脅安全等級，容易而客觀的配置偵測節點。

關鍵詞: 入侵偵測系統、納許均衡、夏普利值、安全風險值、威脅安全等級。

一、緒論

電腦網路交易頻繁而弱點日益浮現，網路攻擊類型漸漸朝向自動化，入侵手法亦趨向複雜化。成功的網路攻擊足以癱瘓線上交易市場，企業於是設置入侵偵測系統來減低攻擊帶來的破壞。現行企業或組織在面臨網路攻擊的威脅下，紛紛建立「安全監控中心」(security operating center)及「區分威脅等級」的警示系統，以提供資訊安全應變機制，例如：賽門鐵克網路威脅分級系統 ThreatCon Level [15]，但沒有一個具體數學模型可以解釋攻擊及防衛者間的互動關係，並且能依據分級模型作客觀合理的分配。本研究

希望能夠用賽局理論中的均衡概念來提供一個穩定的架構，有效率的解決偵測節點配置的問題。

現行的入侵偵測系統區分兩種：事前的預防（例如：安全的覆蓋網路或代理網路服務等等）與事後的補救（例如：異常軌跡偵測或惡意封包過濾等等） [6][8]，安全的覆蓋網路服務(secure overlay services: SOS)可以預防並前瞻性的減輕分散式阻絕服務攻擊(distributed denial of service)，但是偵測節點間互相聯繫產生大量的負荷，而限制其架構的擴充性。雖然安全的覆蓋網路服務較事後的補救方法有效，但是它存在配置節點效率上的問題：需要多少偵測節點配置在入侵偵測系統上較有效率？以及那些是抵抗攻擊的最重要反制節點？

入侵偵測系統管理者經常面臨一個難以決定的問題：在一定的成本下，運用多少的偵測節點可以有效的防護網路安全？配置（曝露）愈多的節點反而容易被攻擊者滲透利用，並且付出較多的成本。大量的配置偵測節點，密集的相互協調，容易讓安全出現漏洞，所以一個強固完善的分散式入侵偵測系統，必須在網路的安全性和配置偵測節點之間，取得一個較佳的平衡。這情形就如軍隊作戰時，指揮官必須配置有生命的（人員）與無生命的（武器、裝備）資源在戰場上，首先考量敵人的位置、兵援、武力及攻擊程序..等等。然後，檢查自已的優勢及弱勢作戰位置，最後根據敵方的最優勢策略作出自已的最佳策略。在過與不及的防衛配置中，考量雙方策略後找到優勢的策略。

賽局理論爲多人競爭和彼此互動提供分析行爲的重要工具 [5]，我們從攻擊的模型來量化提出的架構，以診斷網路安全的風險（攻擊的威脅），並適時的決定偵測節點的配置。現行最佳化方法難以解決成本配置的問題 (Cost Allocation Problem) [17]，本研究嘗試從賽局均衡的角度著手研究，提出因應威脅等級的配置架構（Threat Condition Deployment using Game Theoretic Approach: TCDGT），這架構可以在網路受到不同的威脅時（例如：強烈威脅時及威脅程度減弱時）做出穩定（stability）而有效率的合理選擇，經由配置偵測節點的優先順序，建置經濟而均衡的入侵偵測系統。

本研究提出兩步驟的賽局模型，首先，第一個模型將網路攻擊者與偵測節點間的互動過程對應在一個非零和、雙人與非合作的賽局中，根據雙方提供策略的測量安全因子（例如：偵測率、誤判率或頻寬消耗率等等），建構雙方的支付函數(payoff function)，之後再利用這些函數算出雙方的混合策略均衡點(mixed strategy Nash equilibrium)，當作一個偵測節點的安全風險值(security risk value)。接著，第二個模型在安全覆蓋網路的入侵偵測系統中，將所有偵測節點建構成一個合作賽局，根據每節點安全風險值，平均區分多個「由強到弱」的威脅安全等級，並且應用強而具有指標性的夏普利值(Shapley value) [13]來計算一個彼此均認可的成本配置集合，如此可以結盟(coalition)各安全等級的節點，並算出各節點的邊際貢獻(marginal contribution)。我們以此建立一個評比系統，產生偏好尺度來估計整體的效用及期望作爲決策依據 [9]，它可以根據在不同的安全警示等級下（或不同成本考量），經濟而有效率的選擇偵測節點來擔任防禦的任務。

爲了驗證提出架構可行性，我們假設有20個偵測節點的數據，計算它們的安全風險值，並平均區分四個威脅安全等級（綠燈、黃燈、橙燈、紅燈），最後得到四個等級的夏普利值配置集合。數據顯示：如果選擇不同的燈號（呈現不同的攻擊程度），就會產生不同的夏普利值，因此顯示出來它的邊際貢獻，以提供決策者一個客觀判斷的標準(scale)。

本文的組織結構如下：第二節我們介紹賽局理論應用在網路安全方面的相關研究。第三節我們設定本研究入侵偵測系統的安全覆蓋網路。第四節提出系統配置的架構，並依序介紹安全風險賽局和配置偵測節點賽局。第五節我們計算假設的數值來評估架構的可行性。第六章做出結論並指出未來的研究方向。

二、文獻探討

賽局理論可以把它看成多人決策理論，它提供一種語言去制定、建構、分析及預測參賽者間互動(interaction)決策的過程。這種策略思考是透過推估，找出合於自已的最大勝算，以利在競爭中獲利 [5]。賽局理論劃分合作賽局及非合作賽局兩部份，它們考量的元素有以下：一個賽局必須超過一個以上的參與者。每個參與者和其他參與者具有互動策略（行動）。參與者是否可以明確得到這些策略訊息？雙方互動結果會產生一個支付函數(payoff function)，這函數可以呈現每參與者的偏好。

近年來，電腦網路入侵偵測領域裏，應用許多賽局理論的方法去建構攻擊者與防衛者之間的互動關係。Cavusoglu [3]等學者認爲IDS面對駭客的攻擊及自身的防禦策略考量下，是一種檢查賽局（Inspection game），它和核武裁減協定的賽局相似，與我們所提出的模型類似。他們研究入侵偵測系統及網路使用者影響賽局模型的參數及變數，利用機率混合策略算出最適反應函數，並利用向後推導(backward induction)方式算出IDS和使用者的納許均衡，以找出最佳策略。該研究發現：IDS的偵測值最佳化是取決於使用者的「入侵系統的操作容易度」和「壓制攻擊的方法」，兩者比提昇IDS的偵測技術還要來的重要。該研究缺點是在設定參數時，並不能滿足當時IDS的模組實際狀況，比較有IDS及沒有IDS的結果，只滿足少部份管理方面的需求。

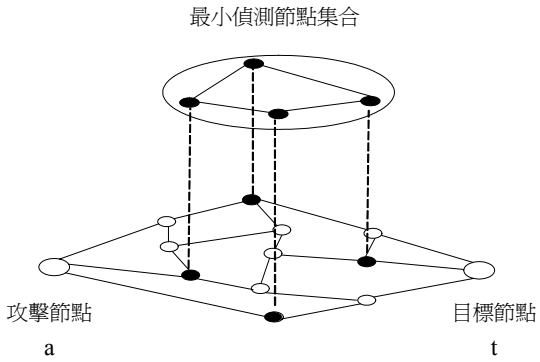
Alpcan [1] 等學者用兩個賽局模型去解釋網路攻擊者和入侵偵測系統間的互動關係。第一個模型是用多人的合作賽局，建構安全的偵測警示系統(Security warning system)，讓管理者可以在入侵偵測系統(IDS)的誤判率(false alarm)和漏判率(missing intrusion)之間做適當的權衡，它主要是給定三種不同門檻值（紅、黃、綠燈警示）並利用夏普利值(shapley value)計算出各節點的資源分配強度，以提供管理者可以權衡、選定那些是優先的偵測點(sensor)。第二個模型是將攻擊者與IDS的行爲對應在一個雙人非合作及非零合賽局，用機率混合策略(mix strategy)算出均衡解。該研究有以下的缺點：第一，用夏普利值(shapley value)計算偵測節點分配最佳化，並未說明提供管理者決策的意涵。第二，該模型在攻擊者和入侵偵測系統行爲的描繪過於簡略，應該考慮更多影響賽局的變數，例如擴散攻擊方式、網路流量等等，才能使得模型更符合現實。本研究具有一個優點：Alpcan 的研究只提出兩個互爲獨立沒有關聯的架構，而我們將兩者的模型考量更完善，將兩者整合並提出一完整的架構，作爲量測安全與分析、決策的模型。我們亦考慮攻擊者與偵測節點的真實策略產生的結果，確實的整合安全風險模型與入侵系統的配置模型，作爲決策者一個有效率的配置方法。

如果考量有限成本，本研究是第一個提出配置入侵偵測系統的架構，偵測節點的成本配置問題是一個非多項式(NP-Complete)可以解決的問題 [7]，目前計算公平的成本分配有電力傳輸系統及網路多點傳輸系統，Zolezzi [17]等學者發現利用夏普利值計算方法比傳統的解決方法還經濟有效。因此，我們參考Owen [13]提出的簡化夏普利值計算方

法，將每個偵測節點的安全風險值，平均分配多個警示程度，這種配置的解決方案提供網路威脅安全等級防護公司，一個有效的度量方法。

三、安全覆蓋網路

本研究假設入侵偵測系統的安全監控中心配置一些重要偵測節點，來管理與監控整個大型網路。如在圖一中，入侵者在網路中選定一條從攻擊者 a 到目標者 t（受害者）的路徑來傳送惡意封包，IDS配置自主的節點或代理人（agent）來監視或報告入侵異常事件，它的集合爲$N = \{n_1, n_2,\ldots, n_N\}$，這些節點具有簽章比對、偵測惡意封包及統計分析的功能，然而這些節點被一些安全因子（例如：偵測率、誤判率及頻寬消耗比例等等）互相影響。本研究的架構由這些安全因子計算出各節點的安全強度（SRV），再依各種不同的威脅安全等級，用夏普力值(Shapley value)計算各節點群聚(aggregation)程度，並公平的算出不同等級的節點配置集合。因此管理者可以決定：在不同的等級中，選出抵抗攻擊的節點集合，$P^h=\{n_1^h,n_2^h,n_3^h,...,n_i^h\}\forall_i \in N$，$h$是不同的威脅安全等級（例如：綠、黃、橙、紅四個等級）。



圖一: 最小偵測節點集合的安全覆蓋網路

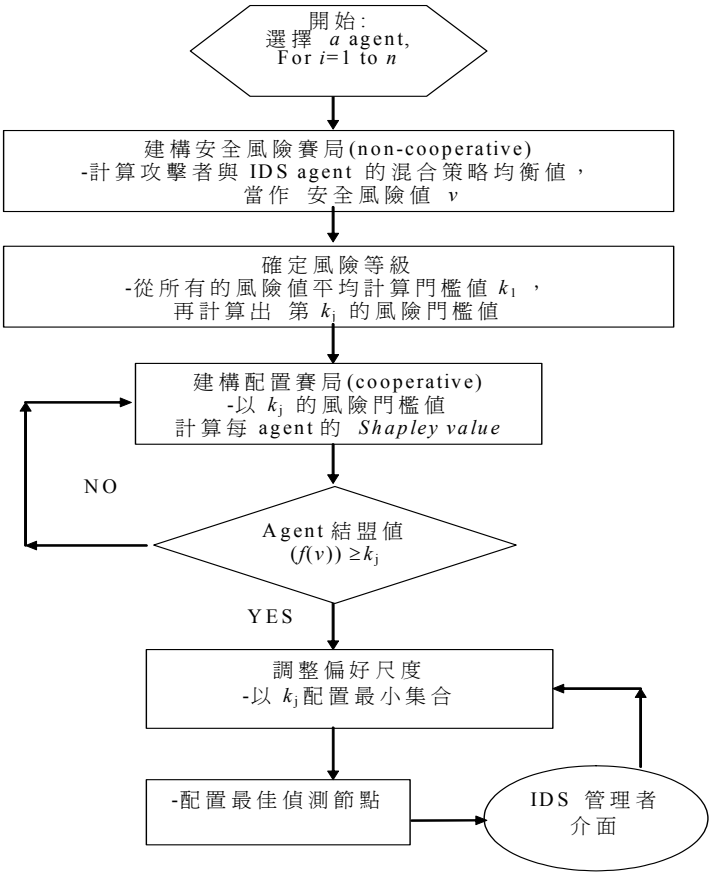
四、TCDGT架構

本研究提出一個應用賽局理論，並依威脅安全分級來配置網路入侵偵測系統的安全覆蓋網路架構。在圖二中描述整個架構的運作流程，這架構用兩階段的賽局來建構經濟而有效率的節點分配。第一階段我們用雙人、非零和及非合作的安全賽局，去探究攻擊者與偵測節點間的行爲，找出它們之間的風險因子，將其對應到一個報酬矩陣(bi-matrix)，並算出每個節點與攻擊者間的納許均衡點(Nash Equilibrium: NE)，來當作節點的安全風險值SRV。第二階段將所有節點想定爲合作配置賽局，用各節點SRV值平均計算節點的威脅安全門檻值，以便於律定出整個IDS的安全等級，並依安全等級計算夏普利值，形成一個強力指標，能夠容易的建構公平及有效率的IDS節點配置，這使得決策者可以選定最適化節點來配置安全的覆蓋網路。最後的程序可以增加或減少可調整的量尺(preference bar)，動態的配置合適IDS節點。

1. 安全賽局

每個節點遭受破壞程度及發生的頻率（比例）定義爲安全風險(security risk)。安全破壞(security breach)是在一個資訊系統中，攻擊者能夠成功的破壞有形與無形的資產。所以安全風險量測是由「影響或破壞的事件（安全測量因子）中失去或得到的成本(cost)」與「其發生事件的比例」相乘得到 [14]。我們可以定義安全風險效用如下：

安全風險效用＝∑(影響或破壞的事件的比例×每個事件失去或得到的成本)



圖二: 兩個賽局模型提供最佳化配置的流程

第一個賽局模型的主要目的是捕捉攻擊者及節點間的行爲，我們將其對應在一個雙人非合作賽局，以利得到節點的SRV，這種安全度量的方法是以敵人的觀點著手，它可以補足IDS節點單一觀點的防禦方法，以下分別說明雙方的安全測量因子：

攻擊者(attacker)：我們提供的網路架構中，所有的使用者被IDS所監控，使用者會因爲好奇心、同儕自我炫耀或摧毀意圖等等因素轉變成網路攻擊者 [15]，如果他發動攻擊而未被偵測到，因此獲得利益，所以他付出的成本爲$-b_2$；如果被偵測到，他必定付出懲罰性的成本b_1，攻擊者的效用值(utility)如果是 $(b_1-b_2)\le 0$，代表是獲得正面的效用；如果是 $(b_1-b_2)\ge 0$，代表是負面的效用。我們定義攻擊者可以發動擴散攻擊及單純攻擊兩種：擴散攻擊可以滲透IDS節點，迅速地把惡意碼擴散到其它節點(例如：DDoS 和 code red worm）[18]；相對地，單純攻擊只是單一事件，不會擴散病毒或惡意碼。所以當攻擊者發動擴散攻擊時它的擴散率爲 l_i，還有我們假定網路的存取容易度和攻擊是有關聯性，因此，設定 f_i 是在第i^{th}節點的網路使用頻寬比例。我們假設頻寬使用比例增加，

攻擊的可能性亦隨之增加；如果降低，攻擊亦降低，面對純粹的攻擊參數爲f_i ，如果是擴散攻擊時，參數爲λf_i，λ設定爲倍數。

$M_a :=$

Attack's strategies	Agent's strategies		
	Detection (d_1)	No-detection (d_2)	*q-mix*
Pure attack (u_1)	$b_1 f_i$	$-b_2 f_i$	$b_1 f_i q - b_2 f_i (1-q)$
Propagation attack (u_2)	$b_1(1+\lambda f_i + l_i)$	$-b_2(1+\lambda f_i + l_i)$	$b_1(1+\lambda f_i + l_i)q - b_2(1+\lambda f_i + l_i)(1-q)$
No-attack (u_3)	0	0	0

$M_d :=$

Attack's strategies	Agent's strategies	
	Detection(d_1)	No-detection (d_2)
Pure attack (u_1)	$c_1(1+p_d+m_i)$	$c_3(1+(1-p_d))$
Propagation attack (u_2)	$-c_1(1+p_d+l_i+m_i)$	$c_3(1+l_i+(1-p_d))$
No-attack (u_3)	$c_2(1+p_f+m_i)$	0
r-mix	$-c_1(1+p_d+m_i)r_1 - c_1(1+p_d+l_i+m_i)r_2 + c_2(1+p_f+m_i)(1-r_1-r_2)$	$c_3(1+(1-p_d))r_1 + c_3(1+l_i+(1-p_d))r_2$

(1)

IDS 節點(agent)：偵測節點是檢查使用者的交易紀錄，來判斷他是正常者或是攻擊者?Keromytis [8]等學者利用SOS架構，定時的更新安全覆蓋網路偵測節點的組態，以利防禦網路攻擊的擴散。因此，這裏我們設定 m_i 爲IDS節點 n_i 從一個主機移動到另一個主機的移動比例。節點偵測會產生漏判率及誤判率兩種錯誤：把攻擊者誤認爲正常使用者(false negative or miss attack)和把正常使用者當作爲攻擊者(false positive or false alarm)，接收操作特徵曲線(ROC)可以描述它們之間的關係，如果IDS節點有高的偵測率，隨之也會產生高的誤判率，ROC曲線可以呈現出誤判率與漏判率的權衡關係 [3]，因此，我們給定每個節點的偵測率爲 p_d，漏判率爲$(1-p_d)$，誤判率爲 p_f，節點偵測到攻擊付出成本爲 $-c_1$，漏判率付出的成本爲 c_2 ，誤判率爲 c_3。

本研究建構攻擊者及偵測節點兩人賽局的混合策略表示式(normal form game)如下：1.參與者（players）集合：{攻擊者(attacker)，偵測節點(agent)}。2.策略集合：$\{S_{\text{attacker}}, S_{\text{agent}}\}$, $S_{\text{attacker}} = \{u_1, u_2, u_3\}$; $S_{\text{agent}} = \{d_1, d_2\}$ ，u_1代表單純攻擊策略，而它的混合策略發生機率爲 r_1；u_2 代表擴散攻擊，它的混合策略發生機率爲r_2；u_3代表未作任何攻擊，它的混合策略發生機率爲$1-r_1-r_2$。d_1代表節點有偵測到攻擊並給予適當回覆的策略，它的混合策略發生機率爲 q，d_2代表未偵測到攻擊，它的混合策略發生機率爲$1-q$。有了以上的定義後，我們利用上述安全風險效用的定義，設定雙方的報酬矩陣(bi-matrix) (M_a, M_d) 如方程式(1)，並擴充這矩陣，加上一欄及一列來表示混合策略，偵測節點的混合策略爲 *q-mix* ，攻擊者的混合策略爲*r-mix* [5]。

我們假定雙方是理性的，雙方的策略資訊是透明，他只有考慮對手的支付函數，而不是自已的支付函數最佳化。我們假設：在這安全風險的賽局中沒有純粹策略均衡。所以我們用純粹策略的機率分佈，來訂定他們的混合策略。由於參賽者的選擇具有不確定性，混合策略納許均衡產生是按照發生機率呈現出一穩定的狀態。

如果在報酬矩陣中，分別滿足以下兩個不等式，我們可以用避免利用法（prevent-exploitation method）得到一組雙方的混合策略均衡值(r^*, q^*) ：[2][5]

$[q^*(-c_1(1+p_d+m_i)r^*_1-c_1(1+p_d+l_i+m_i)r^*_2+c_2(1+p_f+m_i)(1-r^*_1-r^*_2))+(1-q^*)(c_3(1+(1-p_d))r^*_1+c_3$
$(1+l_i+(1-p_d))r^*_2)] \le [q(-c_1(1+p_d+m_i)r^*_1-c_1(1+p_d+l_i+m_i)r^*_2+c_2(1+p_f+m_i)(1-r^*_1-r^*_2))$
$+(1-q)(c_3(1+(1-p_d))r^*_1+c_3(1+l_i+(1-p_d))r^*_2)],$
$r^*(b_1f_iq^*-b_2f_i(1-q^*))+(1-r^*)(b_1(1+\lambda f_i+l_i)q^*+b_2(1+\lambda f_i+l_i)(1-q^*)) \le r(b_1f_iq^*-b_2f_i(1-q^*)$ (2)
$+(1-r)(1+\lambda f_i+l_i)q^*+b_2(1+\lambda f_i+l_i)(1-q^*)),$
$r^*[b_1f_iq^*-b_2f_i(1-q^*)] \le r[b_1f_iq^*-b_2f_i(1-q^*)],$
$r^*[b_1(1+\lambda f_i+l_i)q^*-b_2(1+\lambda f_i+l_i)(1-q^*)] \le r[b_1(1+\lambda f_i+l_i)q^*-b_2(1+\lambda f_i+l_i)(1-q^*)]$

$0 \le r^*,\ q^* \le 1$. 雙方的混合策略均衡值是最佳化策略，可以得到 $r^*_i=\{r^*(u_1), r^*(u_2), r^*(u_3)\}$ $q^*=\{q^*(d_1), q^*(d_2)\}$。我們設定第 i^{th} 個偵測節點的安全風險值SRV爲 v_i ，它代表偵測與攻擊的機率，由以下方程式(3)可求出：

$$v_i = \frac{r_i^*(u_1)+r_i^*(u_2)}{r_i^*(u_3)} + \frac{q_i^*(d_1)}{q_i^*(d_2)} \qquad i \in N \tag{3}$$

$r_i^*(u_1)$ 和 $r_i^*(u_2)$ 分別代表單純攻擊及擴散攻擊的最佳混合策略機率，$r_i^*(u_3)$代表未攻擊的最佳混合策略機率； $q_i^*(d_1)$代表第i^{th} 節點的最佳混合策略偵測機率，$q_i^*(d_2)$代表最佳混合策略未偵測機率，因此我們把兩者的比例相加，以 v_i 表示雙方的最佳混合策略機率，這數值代表SRV的強度。下節我們將用這數值代表合作賽局裏特徵函數的元素，來計算每個節點的夏普利值。

3. 配置賽局

這節我們假設在IDS的安全覆蓋網路中，每個偵測節點在進行一場合作賽局，管理者必須決定：考量有限的成本下，要安排那些節點可以達到最經濟的效果？因此，我們需要一個公平及有效率的方法，可以排定他們的優先順序。近年來有許多學者應用夏普利值的計算方法，來作公平的成本分配 [12]，尤其應用在傳輸系統中非常的多，而這些研究也證明傳統的配置系統沒有像夏普利值的計算如此有效，而且它也滿足許多公平必須考量的特性 [17]，因此，本研究應用夏普利值的計算方法，來產生最佳化入侵偵測系統的配置模型。

我們定義一對一的特徵函數 y: $V \rightarrow \mathrm{R}^+$，在所有的元素 v 中，對應成正實數，例如 $y(0)=0$。假定IDS是以 H 個威脅安全等級來配置節點 $H=\{h_1,\ldots, h_H\}$，分別用門檻值 $0<k_1<k_2<\ldots<k_H$(threshold values)爲區分。換句話說，給定所有節點的 SRV 數值，如果 IDS 中所有節點的 SRV 值總和大於及等於門檻值 k_j，我們就說此網路目前處於 h_j 安全等級狀態。我們設定所有的安全等級 L，如方程式(4)，它表達出 h_j ， k_j 和各 y 函數值之間的關係：

$$L = \begin{cases} h_1 & \text{if } \sum_{i=1}^{N} y(v_i) \ge k_1 \\ h_j & \text{if } \sum_{i=1}^{N} y(v_i) \ge k_j \\ h_{j+1} & \text{if } \sum_{i=1}^{N} y(v_i) \ge k_{j+1} \\ h_H & \text{if } \sum_{i=1}^{N} y(v_i) \ge k_H \end{cases} \tag{4}$$

$$\text{令 } k_1 = \left(\frac{v_{Max} - v_{Mini}}{H+1} \right) \tag{5}$$

所以方程式(4)中 $k_j=2k_1, k_{j+1}=3_{,\ldots,}k_H=Hk_1$

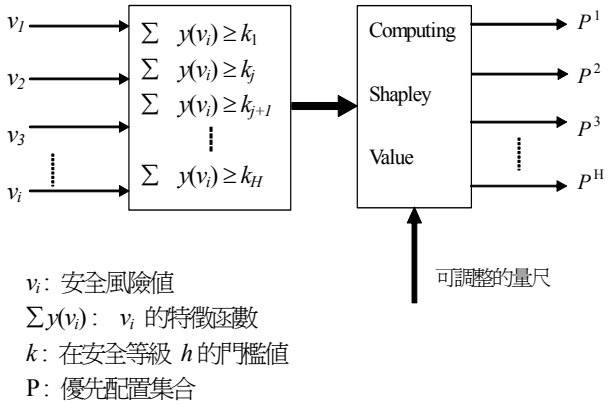
當我們將網路依照方程式(4)和(5)把安全等級分成H級後，接下來的問題是如何在成本有限的情況下，以最佳的方式來配置這些偵測節點？爲了回答此問題，我們可以將這些節點的SRV值，模式化成一個N人的合作賽局，所有參賽者（節點）集合爲 $X=\{1, 2,\ldots, N\}$，當$V\subset N,\ v_j\neq 0,\ \forall_j\in V, V=\{v_1, v_2,\ldots,v_j\},\ j\in n$，在$N$中所有參賽者的次集合，就是一個結盟(coalition)[10][13]，所以在k^{th}門檻值的安全等級下的結盟是X 的次集合，因此，我們可以依據不同的安全等級呈現出不同的威脅型態(threat pattern)。

我們設定特徵函數：結盟C的群聚值是所有節點SRV (v_i)的加總 $\sum_{i\in C}y(v_i)$，每一個節點屬於一個或多個安全等級中的門檻值，我們就可以根據不同的安全等級，應用夏普利值的計算方法算出不同的配置節點。由於不同的入侵威脅安全等級，可以反應出每個節點對於其它節點的相對重要性，設定$y(C)=\sum_{i\in C}y(v_i),\ v_i\in V$, $C\subset X$，c是結盟C的基數。因此，我們可以用方程式(6)計算第i^{th}個節點的夏普利值輸出向量。

$$S(i):=\sum_{\substack{C\subset X\\ i\in C}}\frac{(c-1)!(n-c)!}{n!}[y(C)-y(C-\{i\})] \tag{6}$$

$$\Rightarrow S(i):=\sum_{C'\subset X}\frac{(c-1)!(n-c)!}{n!} \tag{7}$$

爲決定第 i^{th} 節點的SRV是否大於等於第h^{th}安全等級的門檻值時，方程式(6)可以簡化成方程式(7)，如果「大於等於」不成立 $y(C)$-$y(C$-$\{i\})$ 這部份產生0，如果成立就產生1的結果，代表在這些節點SRV總合大於等於門檻值 k_j ，而達到一個成功結盟C'(winning coalition)，$\sum_{i\in C'}y(v_i)\geq k_{\mathrm{j}}$ ，所以可以簡化成方程式(7)的夏普利值 $S(i)$ 。



圖三: 利用夏普利值產生節點配置的流程

我們以圖三的流程來表示：當所有節點的SRV輸入後，會依據不同的門檻值計算各節點的夏普利值集合，這集合以估計期望效用爲基礎，可以作爲一個配置IDS節點的

評比系統。管理者還可以利用可調整的量尺，動態的選擇偵測節點的最佳集合，以便於縮短遭受攻擊的回覆時間。

五、數值分析

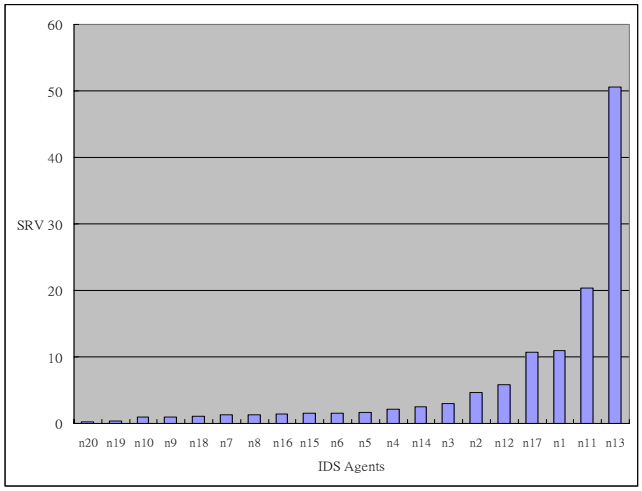
我們假設有20個偵測節點，給定所有在3×2報酬矩陣中，所有變數隨機產生數值，再應用GAMBIT賽局分析工具 [11] 計算這20個安全賽局的混合策略納許均衡值，以作爲20個偵測節點的SRV值，利用這些數值來驗證提出架構的可行性。表一中列出這些數值計算的參數與結果。圖四則依序輸出各節點的SRV值 V = [v_{20}, v_{19}, v_{10}, v_9, v_{18}, v_7, v_8, v_{16}, v_{15}, v_6, v_5, v_4, v_{14}, v_3, v_2, v_{12}, v_{17}, v_1, v_{11}, v_{13}] = [0.252, 0.38, 0.96, 1.009, 1.093, 1.264, 1.283, 1.461, 1.497, 1.589, 1.685, 2.11, 2.538, 2.925, 4.66, 5.799, 10.675, 10.913, 20.367, 50.638]。接著，我們用方程式(5)平均算出4個門檻值k_{green} = 10.08, k_{yellow} = 20.15, k_{orange} = 30.23, k_{red} = 40.31，當作綠、黃、橙、紅4個威脅安全等級的門檻值，最後依據這些門檻值用MATLAB [4]計算各節點的夏普利值（參見圖五）。

表一: 20 組數值產生節點的安全風險值

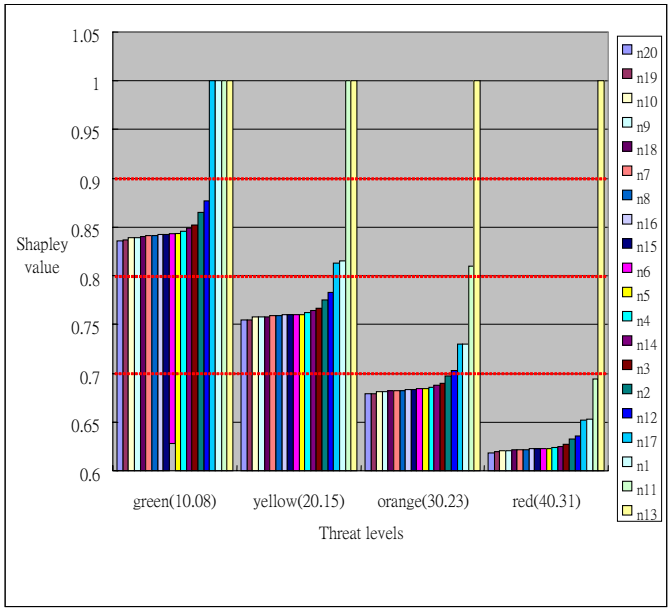
IDS agent	Attacker and agent's parameters										*NE*
	b_1	$-b_2$	f_i%	$-c_1$	c_2	c_3	l_i%	m_i%	p_d%	p_f%	v_i
n_1	10	-100	0.49	-30	80	60	0.8	0.3	0.5	0.5	10.913
n_2	20	-90	0.48	-90	20	10	0.2	0.9	0.9	0.2	4.66
n_3	30	-80	0.4	-80	30	30	0.3	0.8	0.8	0.3	2.925
n_4	40	-70	0.35	-70	40	50	0.4	0.7	0.7	0.4	2.11
n_5	50	-60	0.3	-60	50	60	0.5	0.6	0.6	0.5	1.685
n_6	60	-50	0.25	-50	60	40	0.6	0.5	0.8	0.6	1.589
n_7	70	-40	0.2	-40	70	80	0.7	0.4	0.9	0.4	1.264
n_8	80	-30	0.15	-30	80	60	0.8	0.3	0.8	0.3	1.283
n_9	90	-20	0.1	-20	90	80	0.9	0.2	0.6	0.1	1.009
n_{10}	100	-10	0.05	-10	100	90	1	0.1	0.5	0.2	0.96
n_{11}	5	-95	0.48	-1	99	98	0.05	0.99	0.5	0.1	20.367
n_{12}	15	-85	0.44	-85	15	14	0.15	0.85	0.5	0.1	5.799
n_{13}	2	-99	0.38	-2	98	100	0.99	0.99	0.5	0.1	50.638
n_{14}	25	-55	0.32	-65	35	30	0.35	0.65	0.7	0.2	2.538
n_{15}	100	-10	0.05	-1	100	90	1	1	0.5	0.3	1.497
n_{16}	55	-45	0.22	-45	55	50	0.55	0.45	0.8	0.45	1.461
n_{17}	10	-100	0.49	-30	80	85	0.8	0.3	0.5	0.3	10.675
n_{18}	75	-25	0.12	-25	75	80	0.75	0.25	0.8	0.25	1.093
n_{19}	90	-20	0.1	-85	15	16	0.15	0.85	0.5	0.5	0.38
n_{20}	100	-10	0.05	-90	20	22	0.2	0.9	0.9	0.2	0.252
λ設定爲2。											

在圖五中可以看到綠燈風險等級（安全等級很低）時v_{11}和v_{13}的夏普利值相等，而在紅燈風險等級（安全等級很高）時，v_{11}和v_{13}的夏普利值卻相差很大，所以當IDS設定紅燈時，風險等級高的節點（node）要付出較多的成本去關注；當設定綠燈時，風險等級高的節點可付出較少的成本去關注，應該均分給其他風險等級較低的節點。這符合「捉大放小與防微杜漸」概念，因此解決了決策者的困境。

接著圖五中我們設定有一個可調整的偏好量尺如水平虛線，偏好量尺的意義可以代表不同的網路安全預算，因此當我們由下到上調整量尺，代表預算不同時，分別得到夏普利值大於 0.7、0.8及0.9時的四個配置集合。這些配置集合代表在不同預算，且網路處於不同的網路威脅狀態時，所需配置的網路偵測節點數目可能不同。以下三個實驗結果，我們分析不同安全等級，夏普利值可以公平的計算出成本配置集合（如表二）。



圖四: 20 個 IDS 偵測節點的安全風險值



圖五: 四個威脅安全等級中 20 個 IDS 偵測節點的夏普利值

第一個實驗是調整至最低的水平虛線(Shapley value > 0.7)，當安全等級爲綠燈及黃燈時，所有的節點都配置，橙燈時只配置五個節點$P^{orange} = \{n_{12}, n_{17}, n_1, n_{11}, n_{13}\}$，紅燈配置一個節點$P^{red} = \{n_{13}\}$ 。

第二個實驗是調整至最中間的水平虛線(Shapley value >0.8)，當安全等級爲綠燈時，所有的節點都配置，黃燈時配置四個節點$P^{yellow} = \{n_{17}, n_1, n_{11}, n_{13}\}$，橙燈配置二個節點$P^{orange} = \{n_{11}, n_{13}\}$，紅燈配置一個節點$P^{red} = \{n_{13}\}$。

第三個實驗是調整至最高的水平虛線(Shapley value >0.9)，當安全等級爲綠燈時，配置四個節點$P^{green} = \{n_{17}, n_1, n_{11}, n_{13}\}$，黃燈時配置二個節點$P^{yellow} = \{n_{11}, n_{13}\}$，橙燈和紅燈時都只配置一個節點$P^{orange} = \{n_{13}\}$，$P^{red} = \{ n_{13}\}$。

表二: 四個威脅安全等級中得到三組 IDS 配置

Shapley value >	Threat level			
	P^{green}	P^{yellow}	P^{orange}	P^{red}
0.9	$n_{17}, n_1, n_{11}, n_{13}$	n_{11}, n_{13}	n_{13}	n_{13}
0.8	all	$n_{17}, n_1, n_{11}, n_{13}$	n_{11}, n_{13}	n_{13}
0.7	all	all	$n_{12}, n_{17}, n_1, n_{11}, n_{13}$	n_{13}

本研究中考量各種不同的安全威脅等級並反應出風險的強度，輸出的配置集合比用單純的SRV配置，還來的客觀及有效率，根據數值實驗的結果顯示：在高風險的安全等級中（例如紅燈時），具有高夏普利值的節點比低者，所扮演的角色還重要許多；相反地，而在低風險的安全等級中（例如綠燈時），具有高夏普利值的節點與低者，所扮演的角色並無很明顯的區分。

我們提出的TCDGT架構是一個網路攻擊安全等級警示系統，它可以依據不同的安全等級來觸發配置的策略，管理者可以在網路攻擊的環境當中，用公平而合理的成本，分配給每一個節點。因此，我們的架構可以事先很容易的配置合適的節點來擔任入侵偵測的任務。最重要的是：我們比較圖四與圖五，它能因應各種狀況（安全等級）輸出不同的數值，讓管理者在面對網路攻擊時，能很快的應用動態的調整尺度，快速的找出節點配置的優先順序。它不僅解決IDS節點配置的困境，亦提供現行面對不同威脅狀態的警示機制（例如賽門鐵克網路安全分級系統），一套以量化呈現的方法。

六、結論與未來研究

我們檢視現行防禦網路攻擊的機制，涉及範圍從事後的補救到事前的預防措施，發現最近幾年IDS管理者遭遇到一些困境：如果考量有限的成本，配置多少偵測節點才能有效的防制攻擊的發生？以及使用者存取容易度與偵測節點的功能，如何取捨，才能達到一個合適的配置?本研究提出一個利於IDS決策與分析的TCDGT架構，它包含非合作及合作賽局模型，第一個模型算出偵測節點的混合策略均衡值，當作各節點安全風險值SRV。第二個模型將SRV對應到各種威脅安全等級，算出各節點的夏普利值。爲了建構配置IDS節點的評比方法，我們應用動態可調整的尺度，在安全覆蓋網路中，提供了公平而有效率的入侵偵測系統配置方法。此外，我們用計算20組數值來檢視本研究的可行性，實驗的結果顯示：確實可以將納許均衡與夏普利值兩者的概念整合在一起，提供管理者因應不同的安全威脅時，一套配置偵測節點的優先考量方法。未來希望能應用在SOC中，把各項成本值設定爲固定值（例如$b=c=1$），其它參數用真實的數據來驗證本研究。再者，能夠考量策略的類型及分布的機率，應用貝斯賽局強化我們的模型。

[謝啓]

感謝審稿者能夠撥冗指正本研究，並給予真誠的建議，亦感謝林熙禎老師於網路實驗室的指導，特此致謝。

參考文獻

[1] Alpcan T. and Basar T., "A game theoretic approach to decision and analysis in network intrusion detection", *IEEE Conference on Decision and Control*, 2003: pp. 2595-2600.

[2] Basar T. and Olsder G. J., *Dynamic Non-cooperative Game Theory*, 2nd ed. Philadelphia, PA: SIAM, 1999.

[3] Cavusoglu H., Mishra B., and Raghunathan S., "The Value of Intrusion Detection Systems in Information Technology Security Architecture", *Information Systems Research* 16(1), 2005: pp. 28–46.

[4] Demuth H. and Beale M., *MATLAB Neural Network Toolbox User's Guide*, 4th ed., The Math Works Inc., 2003.

[5] Dixit A. and Skeath S., *Games of Strategy*, 3rd edition, W. W. Norton & Company, 2001.

[6] Ferguson P. and Senie D., "*Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing agreements performance monitoring*", RFC 2827, May 2000.

[7] Goemans M. X. and Skutella M., "Cooperative facility location games", *Journal of Algorithms* (50:2), 2004: pp 194–214.

[8] Keromytis A, V Misra., and Rubenstein D., "*SOS: An Architecture for Mitigating DDoS Attacks*", *IEEE COMMUNICATIONS* (22:1), 2004: pp. 176–188.

[9] Lewis H. W., *Why flip a coin? : the art and science of good decisions*, John Wiley & Sons, 1997.

[10] Lightfoot J.M and Spinetto R.D., "An alternative method to share the initial fixed cost of a local area network", *IEEE Transactions on Engineering Management* (41:2), 1994: pp. 135-142.

[11] McKelvey, Richard D., McLennan, Andrew M., and Turocy, Theodore L., *Gambit: Software Tools for Game Theory*, http://econweb.tamu.edu/gambit.

[12] Mishra D. and Rangarajan B., "Cost Sharing in a Job Scheduling Problem Using the Shapley Value," *Proceedings of the 6th ACM conference on Electronic commerce*, 2005: pp. 232-239.

[13] Owen G., *Game Theory*. 3rd Ed. New York, NY: Academic Press, 2001.

[14] Schechter Stuart E., *Computer Security Strength and Risk: A Quantitative Approach*, PhD thesis, Harvard University DEAS, June 2004.

[15] Shaw D. S, Post J. M, and Ruby K. G., "Inside the minds of the insider," *Security Management* (December), 1999.

[16] SymantecCorporation,<http://www. symantec .com/index.jsp>

[17] Zolezzi Juan M. and Rudnick H., "Transmission cost allocation by cooperative games and coalition formation," *IEEE Transactions on power systems* (41:4), 2002: pp. 1008-1015.

[18] Zou C. C, Gong W, Towsley D., "Code Red worm propagation modeling and analysis," *In: Proc. of the 9th ACM Symp. on Computer and Communication Security*, Washington, 2002: pp. 138-147.