結合軟體代理人及分散式入侵偵測系統應用於國軍網路之研究

作者簡介

丘國富少校，中正理工學院87年班、陸軍通信電子資訊學校通資正規班5期、國防大學中正理工學院電子工程研究所95年班；曾任排長、通信官、採購官、教官，現任職於陸軍通信電子學校。

朱盈豪少校，國防大學中正理工學院87年班、國防大學中正理工學院電研所33期、通資安全正規班13期；曾任排長、連長、教官，現任職於陸軍通信電子學校。

提要

隨著駭客入侵的手法千變萬化，傳統單點式入侵偵測系統（Intrusion Detection System, IDS）已不足以偵測日益精進的入侵手法，分散式入侵偵測系統遂逐漸成為入侵偵測主流，但其在網路頻寬、分散式大規模環境監控、各端點合作溝通能力、警訊誤判及對未知攻擊偵測等方面仍有許多限制，故可利用軟體代理人技術加以改善。本文提出一套以軟體代理人與入侵偵測系統為基礎，適用於國軍網路之架構，用以預防和偵測一些已知和未知的攻擊行為，即時進行動態反應，進而達到網路與資訊系統防護的功能。

關鍵詞：軟體代理人、入侵偵測系統、分散式入侵偵測系統

前　　言

由於網路應用的蓬勃發展，許多以網路為基礎的應用與服務，其中不乏與金融、軍事系統整合的案例，國軍對於網路的依賴與日俱增，因此資訊傳輸及網路環境的安全性，成為相當受重視的課題。入侵偵測系統是近年來相當風行的資訊安全保護機制，具有即時網路安全偵測與回應功能，用來偵測入侵異常行為，負責監控網路環境安全的防衛系統，偵測外部攻擊者以及內部人員對未經授權之資訊系統做不正當的存取或攻擊，能在入侵行為造成危害前發出即時警告，並進行相關反應措施，防範系統遭致破壞。隨著網路環境愈來愈複雜，傳統單點式入侵偵測系統已不足以偵測日益精進的入侵手法，分散式入侵偵測系統遂逐漸成為入侵偵測的主流，但其在網路頻寬、分散式的大規模環境監控、各端點合作溝通能力、警訊誤判及對未知攻擊偵測等方面仍有許多限制，故可以利用軟體代理人技術來加以改善。

本文首先定義何謂入侵偵測系統及軟體代理人，提出一套以軟體代理人與入侵偵測系統為基礎，適用於國軍網路之架構，此架構利用代理人具有自主性、離線作業與異質性分散式處理特性，利用分散式的「監測分析代理人」，對所屬防禦區域的網路環境進行偵測工作，若判定為可疑的封包，則透過「行動代理人」將相關資訊回報到「防衛回應代理人」進行更深一層的偵測與推論動作，同時通知其他的「監測分析代理人」攻擊者的位址及攻擊的型式，「防衛回應代理人」透過其核心「智慧型管理中心」，進行分析、推理及處理更精確的入侵偵測推理、發布警告訊息、評估威脅等級及建立新的入侵規則與反應措施。而「中央控管代理人」則利用全天24小時，全年無休的運作，可以在新的入侵攻擊前，迅速且正確地部署、傳送及啟動防制策略，並以最快的速度提供識別、偵測和清除入侵者的技術給各個「監測分析代理人」及「防衛回應代理人」。

在本文的後段，同時提出本架構系統運作流程、系統功能與模組架構、系統分析方法、入侵等級評估與反應措施，最後針對本研究所提出的架構與目前國外研究最具影響力的兩套美國Purdue大學的Autonomous Agent及AAFID系統作架構比較，希望透過本文提出之架構，使其成為兼具理論與實用之入侵偵測系統，以提供後續研究者參考依據。有關於軟體代理人及分散式入侵偵測系統的研究非常之多，討論的議題也非常廣泛，本文僅整理和探討主題較有關之代表性論點。分述內容如下：

軟體代理人

在網際網路的推波助瀾下，目前軟體代理人被各方頗為看好，針對其所做的研究也日益增加。軟體代理人機制能夠應用於許多領域，通常用來代理使用者處理繁雜的工作，並以合作的機制提升系統執行或管理效率，因此若將代理人的機制有效地應用在大型且複雜的系統，便能節省系統開發的時間並輔助使用者管理物件間複雜的溝通❶。

由於軟體代理人發展至今也不過十幾年，且軟體代理人的應用範圍相當廣泛，

註❶：於下頁。

因此，對於軟體代理人尚未有一個公認的定義，本文藉由以下各學者所做出的定義，來瞭解軟體代理人的特性：

一、Jennings與Wooldridge

Jennings與Wooldridge認為軟體代理人是一個電腦系統，存在於一些環境中，具備自主行為能力應用在各不同環境中，以達成設計目的。軟體代理人必須具備下面三種特性❷：

㈠反應性（Responsive）：代理人察覺環境的變化，即時做出相對應的行為。

㈡主動性（Proactive）：代理人不只是針對環境的改變，而做出回應，代理人會做出具有機會主義（opportunistic）和有目的（goal-directed）的行為，在適當時機採取主動。

㈢社會性（Social）：代理人互動、溝通的能力。藉由與其他智慧型代理人和使用者溝通，以解決問題、達成目標和幫助其他代理人。

二、Wooldridge

Wooldridge於2000年對代理人作定義❸，認為代理人能自主性地進行運作，它能主動察覺環境的變化並採取相對應的動作，本身並擁有特定的技能來執行使用者所賦予它的任務，而所謂的智慧可以是簡單固定的程序或物件邏輯，也可以複雜到具有推論和學習能力。所以通常具備下面幾個特性：

㈠自主性（Autonomy）：代理人不需要使用者直接下指令或是監督，代理人會依據被委託的目標、環境、條件，自主的做出相關行為。

㈡穩定目的（Homeostatic goal）：能反覆針對目標做執行。

㈢適應性（Adaptive）：代理人會根據環境和使用者偏好的改變，做出相對應的調整。

㈣時間連續性（Temporal continuity）：代理人被委以任務，必須不斷地執行，直到任務被使用者或程式終止。

㈤溝通性（Communication）：代理人被交代的任務，可能需要借助到其他代理人的幫忙，以及和使用者的互動，因此，溝通的能力也是必須的。

三、Hess, Rees與Rakes

Hess等人也針對自主性軟體代理人提出定義，自主性軟體代理人是代表或替代個人或是其他代理人，在特定領域中，根據被建置的任務去執行的軟體。而在被建置過程中，基本要包括下面三個特性❹：

㈠穩定的目標（Homeostaticgoal）：穩定目標是當系統到達最終狀況時，也就

註❶：林志敏，〈一個可支援多代理人分散式軟體整合系統建構之代理人樣式語言〉《逢甲大學資訊工程研究所論文》，（2002），頁15～27。

註❷：Jennings, N. R. and Wooldridge, M., Applications of intelligent agents, Agent Technology: Foundations, Applications, and Markets,（1998）, pp.3-28.

註❸：Wooldridge, M. J., Reasoning About Rational Agents,（Cambridge, Mass: MIT Press, 2000）, pp. 10-42.

註❹：Hess, T. J., Rees, P. L. and Pakes, T. R., "Using autonomous agents to create next generation of DSS," Decision Sciences, Vol.31, No.1,（2000）, pp.1-31.

是目標完成時，並不是一個終止的動作；而是繼續去監督，當狀態發生改變時，反覆去執行以維持在最終狀態。

㈡持續性（Persistence）：程式持續不斷地執行以維持穩定目標的目的。

㈢反應性（Reactivity）：可以重新組織環境中的改變，並根據改變及時做出回應的方法。

且Hess等人又認為除了基本的特性外，還有下面三個可以讓代理人更有活力（empowerment）的特性，整個架構如圖一所示。

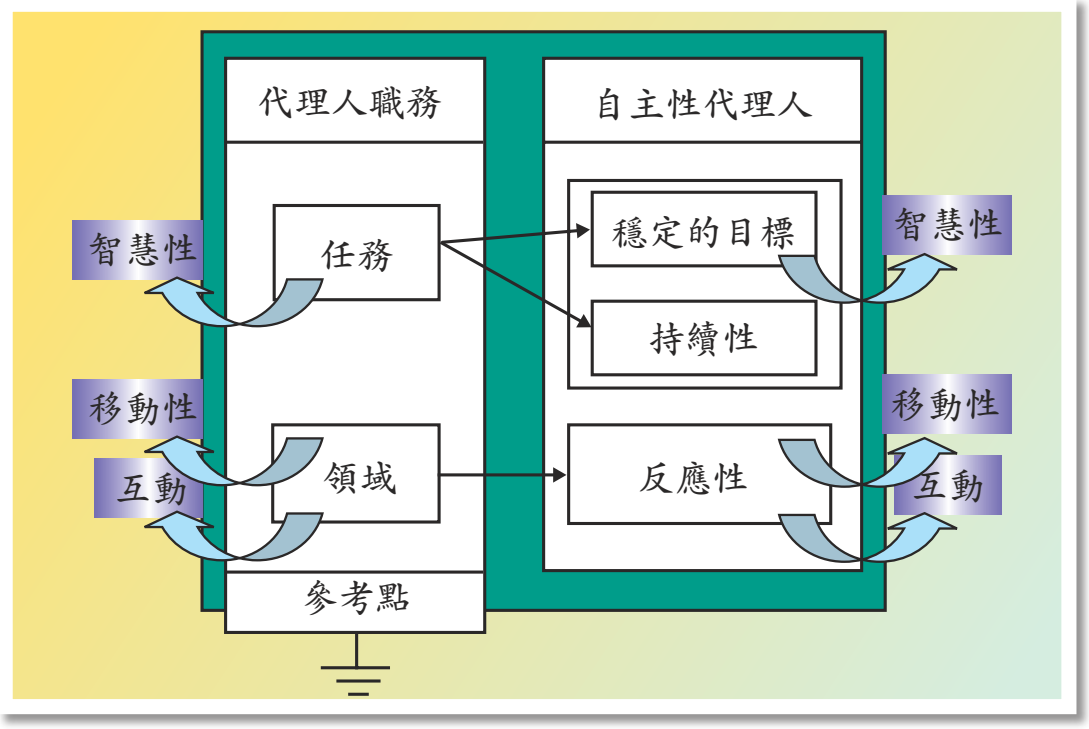
㈠移動性（Mobility）：讓代理人更有效率利用遠端以及網路上的資源。

㈡智慧性（Intelligent）：讓代理人在達成目標的過程中，以較少使用者及設計者的參與，能夠有效率且巧妙地完成任務。

㈢互動（Interactivity）：也就是溝通能力，讓代理人有能力跟使用者或其他代理人程式做溝通，以協同完成任務。

綜合以上的定義，軟體代理人可定義為：「以電腦為基礎的程式，存在於某個環境中，對於環境與使用者偏好的改變，具有察覺、適應能力，而做出相對應的調整，且根據所被交託的目標，主動的、持續不斷的執行，並與其他代理人做適當的溝通，以達成預定的任務。」

由上述可知，雖然軟體代理人乍看之下與一般程式並無兩樣，但事實上與傳統程式最大的區別，在於多了點智慧與自主性，也就是多了幫使用者應付更多事件、處理更多事務的能力。



圖一　軟體代理人架構圖

資料來源：作者繪製

入侵偵測系統

自從Anderson❺於1980年提出入侵偵測系統（Intrusion Detection System, IDS）的技術報告後，入侵偵測系統的研究至今已超過20年。Dorothy Denning❻在1987年首度對IDS模式作定義：「它是一種網路安全監測工具，藉由解讀系統稽核檔或網路封包內容，即時偵測出對系統所進行的攻擊行為，並回報給系統管理者，以加強維護系統安全。」

IDS的目的是要即時且容易的識別由內部與外部滲透者所產生非經允許使用、誤用與電腦系統濫用等可能傷害電腦系統的行為，藉由自動地偵測網路中的封包以檢查出潛在的入侵、攻擊與破壞，以提供最先進的網路防護，其功用不是用來取代原有的各項網路安全機制（如安全身分認證、防火牆等），而是要與他們搭配使用，互補各自不足之處，確保網路傳輸之安全性。

一、入侵偵測系統偵測技術

目前IDS所使用的偵測技術主要分為兩種：錯誤行為偵測及異常行為偵測。前者目前廣泛地被各系統廠商所採用；而後者目前尚在研究階段，僅為少數研究機構以及廠商所採用❼。

㈠錯誤行為偵測

由使用者行為中，找出可能成為攻擊行為的部分，以比對的方式將所偵測到的可疑攻擊行為與系統事先所定義的入侵攻擊模式資料庫進行分析比對，觀察正常的行為，然後定義出正常行為的樣本，當不符合這些樣本時，則視為異常。

㈡異常行為偵測

由網路上發生的事件資訊，找出異於正常行為的行為模式，以識別不尋常的主機或網路運作行為的方式來偵測是否有攻擊行為發生。主要是觀察異常的行為，定義出不正常行為的特徵，觀察攻擊行為不同於一般使用狀態的相異處來進行偵測，當符合所觀察的行為時，則視為異常。這種方式最大的優點是偵測率高，但由於必須得事先定義異常的行為，導致於無法偵測出未定義的攻擊行為。

二、入侵偵測種類介紹

入侵偵測的類型可大致分成「網路型入侵偵測系統（Network-based IDS, NIDS）」、「主機型入侵偵測系統（Host-based IDS, HIDS）」和「分散式入侵偵測系統（Distributed IDS, DIDS）」，各有其優缺點與設置的考量，其各類型介紹如下❽：

註❺：Anderson J. P., “Computer security threat monitoring and surveillance,” Technical Report, Report No. 79F296400,（1980）, pp. 5～15.

註❻：Denning D. E., “An Intrusion Detection Model,” IEEE Transactions On Software Engineering, Vol. SE-13, No 2,（1987）, pp. 222～232.

註❼：劉順德，〈一種以入侵偵測概念偵測郵件病毒的方法〉，Communications of the CCISA，第8卷2期，（2002），頁74～86。

註❽：陳瑞文，〈針對Web應用安全實作之入侵防禦系統〉《國立中正大學通訊工程研究所碩士學位論文》，（2005），頁10～26。

㈠網路型入侵偵測系統（Network-based IDS, NIDS）

網路型入侵偵測系統會針對網路上的連線狀態及傳輸封包的內容進行監控及檢查，以便能偵測是否有攻擊行為正在進行。例如網路型入侵偵測系統能夠偵測出網路上是否有可疑的活動。由於該種模式僅需要在網路上安裝一台偵測主機即可偵測整個網域，因此在管理及使用上較主機型系統來得方便。NIDS大多是監控一個區域網路，根據不同需要部署在網路的各個網段，系統將網路卡設置成混亂模式，可以監聽流過的每一個封包。NIDS的優點是建置成本較低，僅需要一台IDS（PC）即可以監控整個網域，可以減少在每一台主機都安裝IDS所花費的成本。NIDS的偵測範圍也比較廣泛，可以偵測出像DoS（阻斷服務）或Port Scan（通訊埠掃瞄）等攻擊。然而NIDS最大的瓶頸在於網路流量超過NIDS所能處理流量的上限時，就會造成封包遺失的問題，進而影響偵測的準確率。

㈡主機型入侵偵測系統（Host-based IDS, HIDS）

主機型入侵偵測系統必須安裝在欲被保護的主機上，藉由分析該主機上的記錄檔或執行檔以判別是否有入侵或攻擊事件產生。而HIDS主要是建置在重要的伺服器或主機上，針對電腦系統上的重要檔案、日誌檔、甚至是系統呼叫（System Call）進行監控，若本機接收封包後所產生的行為一旦符合入侵規則，HIDS會立即發出警告。HIDS可以偵測出NIDS偵測不到的入侵，例如駭客在受害主機的行為偵測、種植「Back-door（後門程式）」後的系統行為等。在現今攻擊行為氾濫的環境下，電腦科學鑑識已成為日漸重視的議題，而在HIDS可以提供有效的證據保存特性。但是如果同一區域網段內有很多台重要的主機需要被監測時，安裝HIDS所花費的成本相對地提升。網路型入侵偵測系統雖然對網路上攻擊行為的偵測能發揮極大的效用，但是對於利用應用層的安全漏洞進行攻擊的駭客手法就無法發揮偵測與反制的效用，這是它的限制因素。因此，主機型入侵偵測系統便應運而生。

㈢分散式入侵偵測系統（Distributed IDS, DIDS）

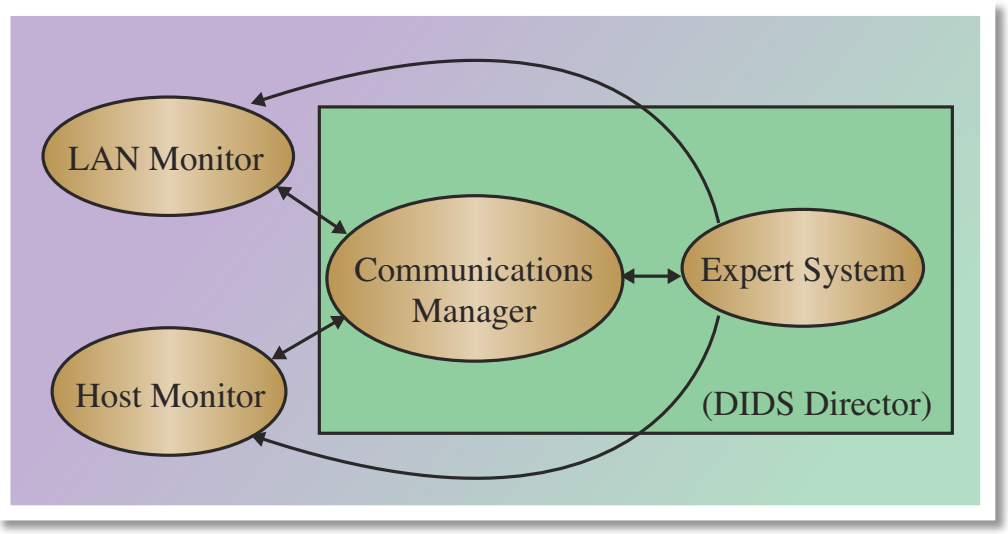
1991年在針對追蹤使用者，在網路上以不同的身分登入進行攻擊行為的想法，設計出標準的分散式入侵偵測系統。其系統架構如圖二，大致上可以分成三個部分：區網監控器（LAN Monitor）、主機監控器（Host Monitor）、分散式入侵偵測系統控制器（DIDS Director）。

㈠區網監控器（LAN Monitor）

區網監控器用來觀察區域網段中主機與主機之間連線的封包流量，並具有描述連線入侵行為的啟發能力，啟發能力是針對每個網路功能、每種服務所需要的認證要求、每台主機的安全設定和過去所發生的攻擊特徵作自我學習並且決定哪些資訊需要傳送給分散式入侵偵測系統控制器裡的專家系統。

㈡主機監控器（Host Monitor）

主機監控器包含主機事件產生器和主機代理人：主機事件產生器負責收集和分析由主機作業系統所產生的稽查資料，還有透過使用者或群組的概括檔（Profile）來追蹤異常行為；主機代理人負責處理所有主機監督器和溝通管理者的通訊。



圖二　IDS分散式系統架構圖

資料來源：作者繪製

㈢分散式入侵偵測系統控制器（DIDS Director）

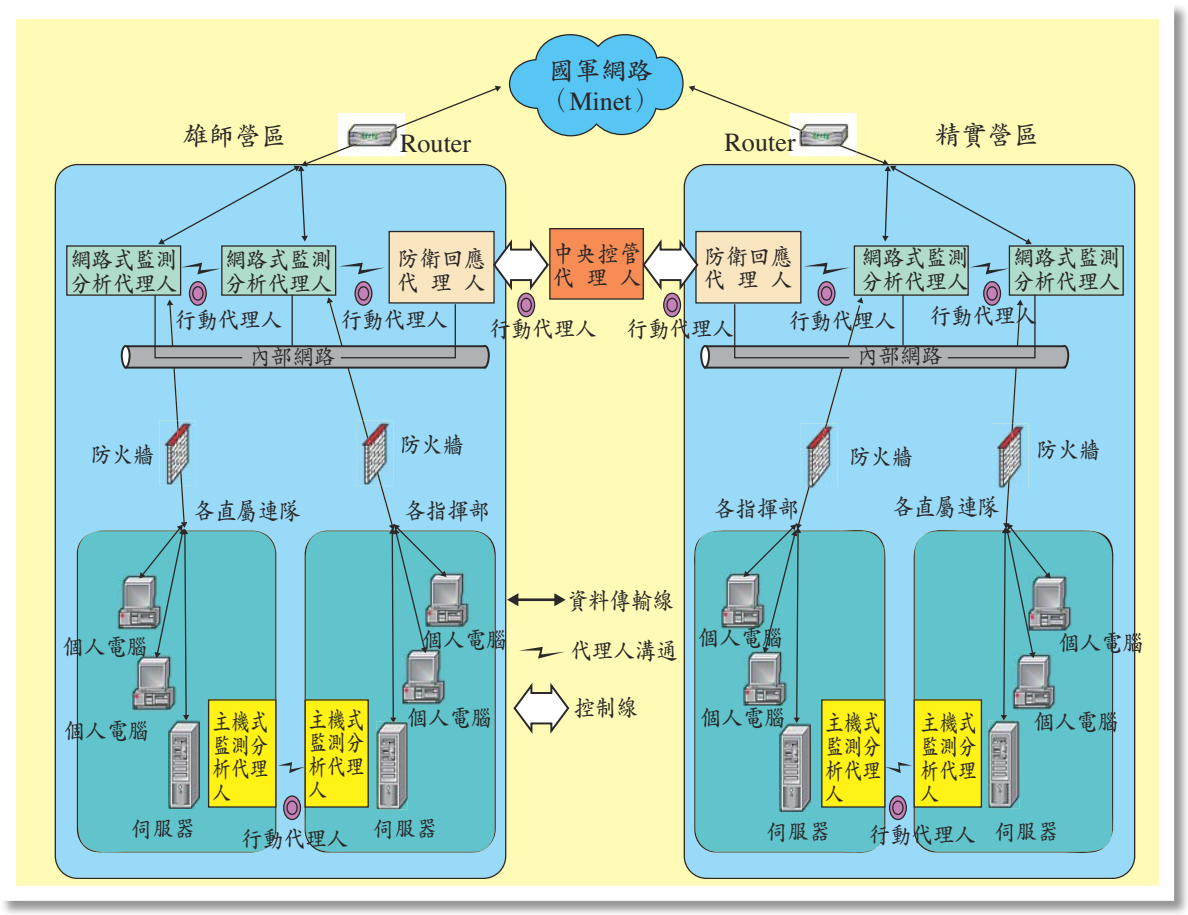
分散式入侵偵測系統控制器主要有兩個元件：溝通管理者——負責傳輸來自區網監控器和主機監控器的資料給專家系統；專家系統——負責接收來自區網監控器和主機監控器的資料。整體來看分散式入侵偵測系統可以達到：偵測網路本身攻擊、偵測涉及多主機的攻擊、追蹤使用者在該網域的移動情形、共用偵測資訊來避免相同的攻擊手法發生在其他主機上❾。

系統架構、運作流程、功能與模組架構

一、系統架構

本文提出一套以軟體代理人與入侵偵測系統為基礎，適用於國軍網路之架構，以國軍內部網路架構為例，列舉雄師營區與精實營區之間應如何溝通合作，即時進行動態反應，達到網路與資訊系統保護的功能，其系統架構如圖三所示。整個系統架構係利用代理人具有自主性、離線作業與異質性分散式處理等特性，對所屬單位內部網路環境部署「網路式監測分析代理人」，對單位內之重要伺服器部署「主機式監測分析代理」，利用分散式的「監測分析代理人」進行偵測工作，若偵測收集的資料經判定為可疑的封包，則透過「行動代理人」將相關資訊回報到「防衛回應代理人」，進行更深一層的偵測與推斷工作，同時也通知其他營區內的「監測分析代理人」，入侵者的網路位址及入侵型態等訊息；「防衛回應代理人」再進一步

註❾：Burroughs D., W. L. and C. G., “Analysis of Distributed Intrusion Detection Systems Using Bayesian Methods,” In Proceedings of IEEE International Performance Computing and Communications Conference, (2002), pp. 41～45.



圖三　系統架構圖

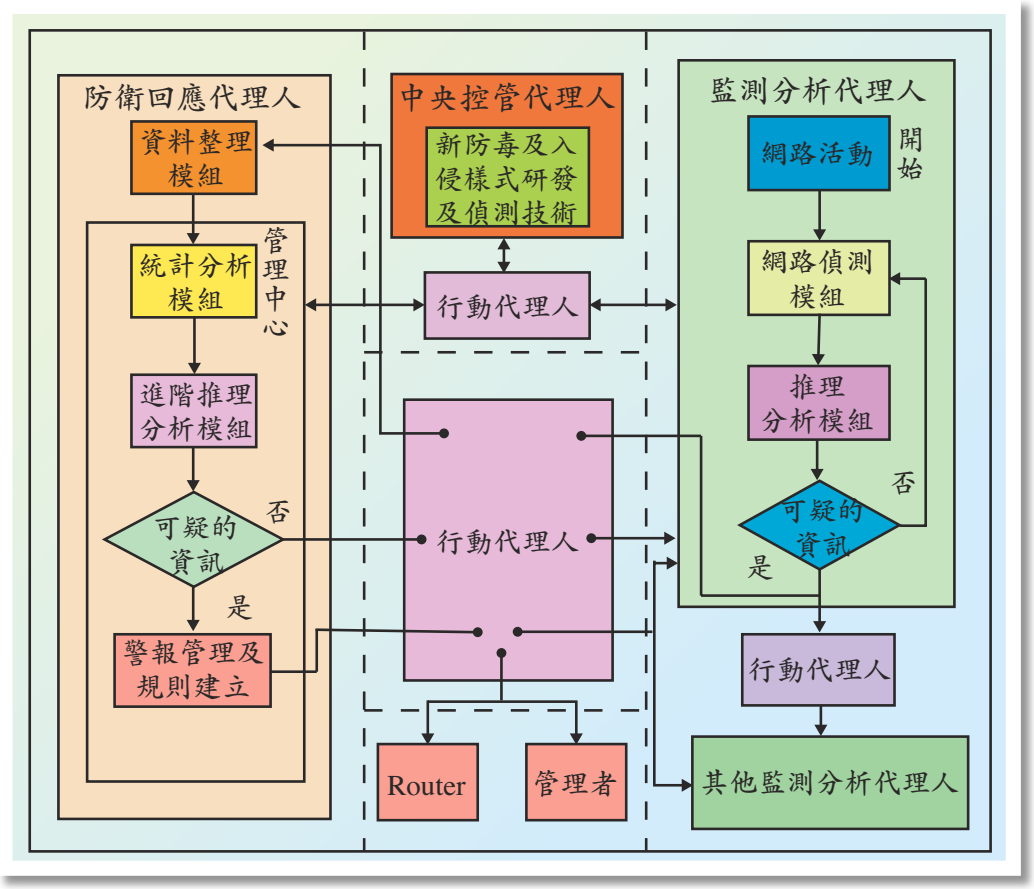
資料來源：作者繪製

的將資訊進行分析、推理、處理更精確的入侵偵測判斷，然後發布警告訊息、比對評估威脅等級、建立新的入侵規則與給予適當的反應措施。而「中央控管代理人」則全天24小時，全年無休的運作，可以在新的入侵攻擊前，迅速且正確地部署、傳送及啟動防禦策略，並透過「行動代理人」溝通，可以將偵測所得的結果回報給單位內的「監測分析代理人」及「防衛回應代理人」，進而達到整體之防範效能。

二、系統運作流程

圖四為進一步闡述「監測分析代理人」、「防衛回應代理人」、「行動代理人」和「中央控管代理人」之間的運作流程[10]，由網路偵測模組進行網路活動的偵測，將偵測收集的資料送入推理分析模組剖析，並與入侵樣式資料庫進行比對；

註[10]：陳培德、賴溪松，〈入侵偵測系統簡介與實現〉《Communications of the CCISA》，第8卷2期，2002年，頁21～37。



圖四　系統運作流程圖

資料來源：作者繪製

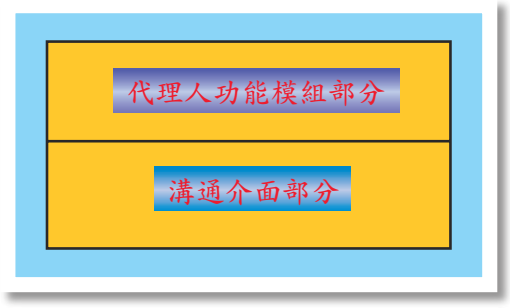
若符合入侵行為樣式，則判定為攻擊之封包，並透過「行動代理人」將相關資訊回報到「防衛回應代理人」，進行更深一層的偵測與推斷工作，同時通知「其他監測分析代理人」，入侵者的網路位址及入侵型態等訊息；「防衛回應代理人」收到攻擊的封包後，透過資料整理模組將資訊解析並管理，再送至「防衛回應代理人」之核心管理中心，經由統計分析模組進行統計分析，再經由進階推理分析模組進一步的推理及進行精確的入侵偵測判斷；若判定為可疑的資訊，則透過警報管理及規則建立模組，與「行動代理人」溝通，發布警告訊息、比對評估威脅等級、建立新的入侵規則與給予網路設備適當的反應措施，同時將相關資訊回報給管理者，以完成第二層防護與管理之用途。「中央控管代理人」則全天24小時，全年無休的運作，可以在新的入侵攻擊前，迅速且正確地部署、傳送及啟動防禦策略，由「行動代理人」溝通，以最迅速的方式將偵測所得的結果，回報給「其他監測分析代理人」及「防衛回應代理人」。

三、系統功能與模組架構

本文所提出的系統主要分為監測分析代理人、防衛回應代理人、行動代理人和中央控管代理人等四種軟體代理人。皆由代理人功能模組部分及溝通介面部分等兩

個部分所構成（如圖五）。

一個軟體代理人通常都會提供一個訊息介面來讓使用者、其他代理人或應用程式與它溝通，透過這個介面，使用者可將要完成的工作交由代理人去完成；相同的，代理人也是經由此介面與外界進行溝通。系統個別所應具備之功能模組部分分別詳述如後：



圖五　軟體代理人構成圖

資料來源：作者繪製

㈠監測分析代理人

可以分為「網路式」及「主機式」監測分析代理人，前者部署於所屬營區防禦之區域網路骨幹上，後者部署於各下轄單位具有特定任務的重要伺服器上，由「網路偵測模組」進行網路活動偵測的工作，將偵測收集的資料送入「推理分析模組」剖析，並與「入侵樣式資料庫」進行比對是否符合入侵行為樣式，若判定為可疑的封包，通過的封包則統計流量及記錄封包，不通過的封包則攔截並發出警告，然後再透過「行動代理人」將相關資訊回報到「防衛回應代理人」做進一步的處理，同時通知「其他監測分析代理人」入侵者的網路位址及入侵型態。

㈡防衛回應代理人

「防衛回應代理人」部署於各營區的網管中心，當「監測分析代理人」在每個受防護的區域端進行偵測後，將偵測過程中的可疑封包資訊回報到「防衛回應代理人」進行更深一層的偵測與推斷工作，透過「資料整理模組」將資訊解析並管理，並由「防衛回應代理人」之核心「管理中心」，進行分析、推理、處理更精確的入侵偵測推理、發布警告訊息、評估威脅等級、建立新的入侵規則與反應措施，以完成第二層防護與管理的用途。

㈢行動代理人

「行動代理人」位於「監測分析代理人」與「防衛回應代理人」之間，負責居中接收、分派與整合任務。它將由「監測分析代理人」所傳遞過來的攻擊資訊透過網路傳遞給「防衛回應代理人」處理，而「防衛回應代理人」亦透過「行動代理人」通知「其他監測分析代理人」採取必要的資訊防護措施，期間所有代理人皆可由「行動代理人」進行溝通及合作，並在發生入侵行為時，立即通知其他成員入侵者的網路位址及入侵型態。

㈣中央控管代理人

為許多智慧型代理人所組成，可委由國防部專責資訊戰及病毒資料庫單位負責，利用代理人自主性、離線作業與學習等特性，作為「監測分析代理人」及「防衛回應代理人」的入侵樣式資料庫的技術支援中心，它必須具有防毒及入侵樣式研發及偵測技術，利用代理人全天24小時，全年無休的運作，可在新的入侵攻擊前，迅速正確地部署、傳送及啟動防制策略，將入侵傷害的衝擊降到最低，即使面對突發入侵事件或是新的病毒，都能做出立即有效的處理，同時必須能夠即時接收及監控全球安全威脅，以最迅速的方式將偵測所得的結果，回報給「其

他監測分析代理人」及「防衛回應代理人」。

四、入侵等級評估與反應措施

本系統經由相關文獻的蒐整，將相似的事件行為群組，依照入侵的嚴重性，分成五個等級，並歸納各等級事件之威脅評估特徵，對相關特徵給予因應之反應措施，將所得的結果與現存的入侵樣式資料庫進行比對，如產生新的結果可包含舊有行為，則以新結果取代之，對於尚未存在的行為，交由專家判斷為正常或異常行為，並透過防衛回應代理人之管理中心回饋訊息到各個代理人，作為偵測及管理用途[11]。

表一為防衛回應代理人接收監測分析代理人所傳送過來的威脅值，並據以採取以下的行動[12]：

結果分析與比較

本文最後將目前國外研究最具影響力的兩套可以將代理人應用於入侵偵測之系統作架構比較，這兩套分別為美國Purdue大學的Autonomous Agent及AAFID系統，首先分析這兩套系統架構特色，再與本文之系統架構比較其功能差異。

一、Autonomous Agent

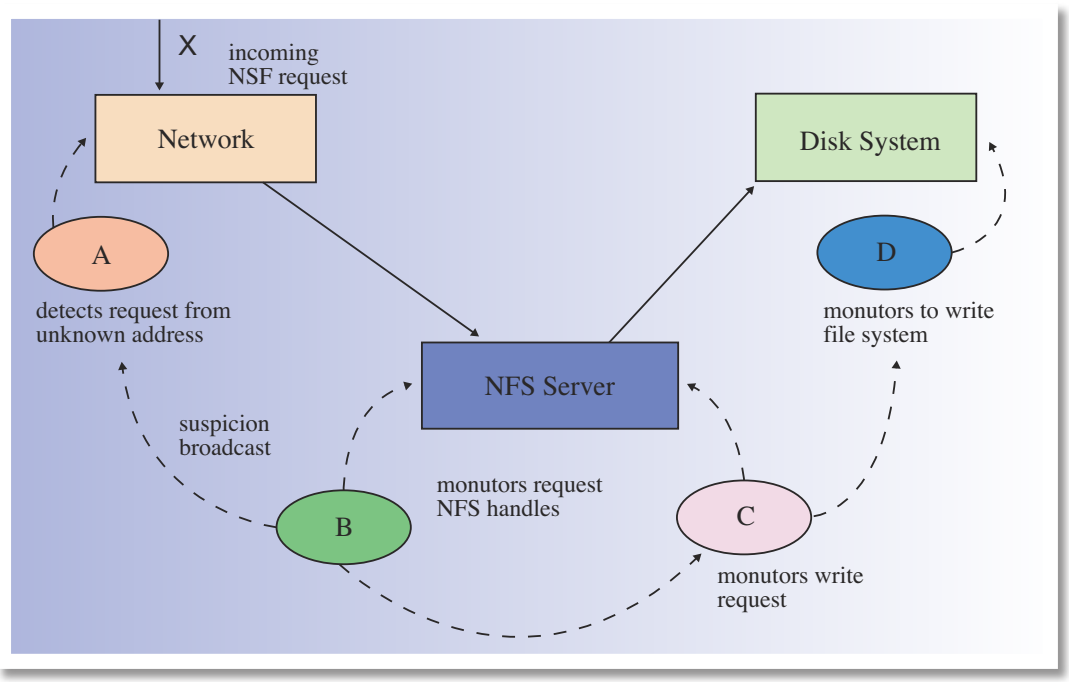
表一　資訊攻擊之威脅評估與反應措施表

威脅等級	威脅評估	反應措施
等級一	屬一般的警戒狀況。	●通知監測分析代理人採用就地的防衛措施即可。
等級二	高於等級一20%的威脅狀況。	●防衛回應代理人加強防衛監測並分析進入者(還無法決定是否為全面性資訊攻擊)的行為模式。 ●通知其他監測分析代理人應加強防衛監測並分析進入者的行為模式。
等級三	高於等級一40%的威脅狀況。	●重新調整各監測分析代理人設定，中斷該次連線，並立即對攻擊來源IP監視。 ●通知其他單位應暫時管制或關閉非緊急的網路通訊。
等級四	整個系統有立即的威脅	●重新設定網路出口端之防火牆及各監測分析代理人設定，禁止攻擊來源IP進入網路。 ●整個系統有立即的資訊系統安全威脅，立即啟動資訊攻擊防衛機制及通報管理者。
等級五	整個系統已全面受到攻擊	●通知整個系統全面啟動資訊攻擊防衛機制並執行資訊易損性評估(遭受攻擊後之更錯、修護能力評估)。 ●通報後，防衛回應代理人立即中斷所有的網路通訊及關閉相關資訊應用系統，宣告全面性的資訊攻擊防衛。

資料來源：作者綜整

註[11]：李駿偉、田筱榮、黃世昆，〈入侵偵測分析方法評估與比較〉《Communications of the CCISA》，第8卷2期，（2002），頁1～5。

註[12]：郭木興，〈以軟體代理人為基，動態資訊防護模式在資訊戰中之應用〉《國防管理學報》，（2001），頁15～30。



圖六　Autonomous Agent圖

資料來源：作者繪製

由美國Purdue大學於1995年提出⓭，該系統由許多分散、自治的代理人程式分別監視網路（或系統）的一小部分，每個代理人程式都包含了一個簡單的感應器、分析器與協調器，彼此透過廣播異常現象來相互合作。圖六為利用Autonomous Agent共同監控NFS的範例，在此範例中A、B、C、D皆為代理人程式，如A監控網路部分，偵測判斷存取NFS的來源位址是否為已知，而C監控寫入需求部分，當A代理人發現過去沒見過的來源位址，就透過廣播的方式通知所有其他代理人提升異常等級，之後若其他代理人也觀察到異常行為，則再度提升其他代理人異常等級。若最後異常等級超過警戒值，則代表有入侵行為發生。

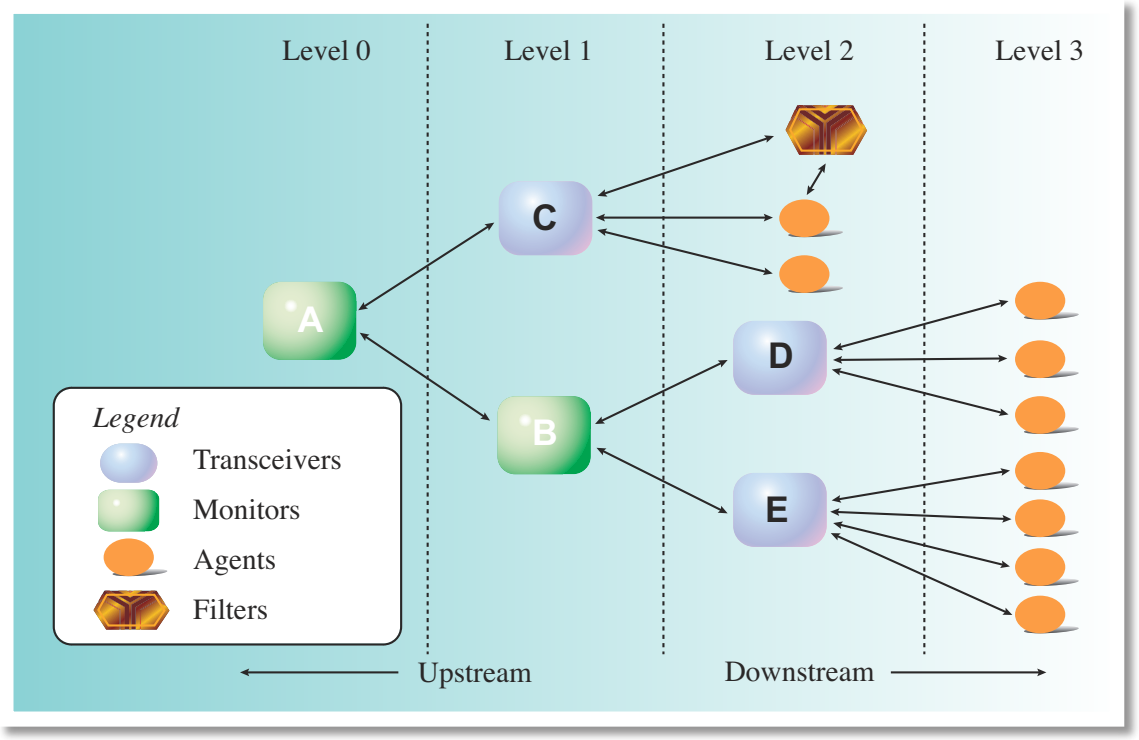
由此系統偵測網路入侵行為的運作模式發現，當代理人程式偵測到異常現象時，無法先行判斷是由那個代理人程式所負責，只能透過廣播方式通知所有代理人程式，並非根據事先定義好的偵測任務進行分派，而是簡單地將網路切成許多分散的小區域，讓代理人程式獨立地監控。

二、AAFID

AAFID⓮由Purdue大學於2000年提

註⓭：Mark Crosbie, Gene S., “Active Defense of a Computer System using Autonomous Agents,” Department of Computer Sciences, 1995, pp. 1～14.

註⓮：Spafford E. H. and Zamboni D., “Intrusion detection using autonomous agent,” Computer Networks, Vol. 34, 2000, pp. 547～570.



圖七　AAFID圖

資料來源：作者繪製

出，是一個代理人式入侵偵測系統的雛型，利用自治型代理人程式的技術，採用階層式的管理架構和報告機制，建立一套分散式入侵偵測系統。圖七為AAFID的系統架構圖，AAFID主要包含四類元件，Agent、Filter、Transceiver與Monitor。一台機器可以放置不限數目的Agent，可以執行特定用途的程式，並將它們所產生的訊息回報給Transceiver，但在AAFID中Agents並不能直接相互溝通。Filters的主要功能為替Agent提供資料選取與資料抽象化的服務，以方便Agent由資料來源處取得所需資訊。Transceiver負責監控所有代理人的運作，可以下達啟動、停止、重設定的指令給代理人。Transceiver同時也將Agent傳回來的資料簡化後，將結果回報給一個或多個Monitor。Monitor為AAFID中最高層的實體，主要負責控制及處理多個主機上的Transceiver（或Monitor）資訊。

基本上AAFID主要目的是建立分散式入侵偵測系統架構，AAFID警示訊息的傳遞主要仍是依循階層式架構進行，各個代理人無法相互溝通，一旦Monitor停止運作，所有受它管轄的傳送器也會停止產生有用的資訊，亦容易產生資料同步性和重複性的問題。

三、系統架構比較

本文利用代理人技術解決分散式入侵偵測系統網路頻寬，降低系統負荷以維持網路的效能，同時利用代理人技術做更精確的判斷，透過持續的運作，允許它們從經驗中學習，並和其他的代理人溝通、協調以及合作，透過分散式的大規模環境監

控，發生異常事件即時處理，避免事態嚴重，在新的入侵攻擊前，迅速且正確地部署、傳送及啟動防制策略，將入侵傷害所造成的衝擊降到最低。

在本系統架構中所提出的系統主要分為監測分析代理人、防衛回應代理人、行動代理人和中央控管代理人等四種軟體代理人，架構特性勢將入侵偵測機制分散於各網路區段中，因此對於新增或移除受保護網路區段，或是一旦網路架構有重大變動，皆可隨之作適當的調整，具有較大的彈性。

在代理人應用於入侵偵測系統之相關研究方面，我們將本系統與Autonomous Agent及AAFID系統，根據其系統架構功能及實際應用情形作一個比較（如表二）。

結　　論

本文將軟體代理人的技術結合至分散式入侵偵測系統架構中，首先介紹軟體代理人之特性、入侵偵測系統之技術與種類，並以簡要的方式介紹本架構的幾個主要組成，包含「監測分析代理人」、「防衛回應代理人」、「行動代理人」以及「中央控管代理人」等，依據本文所提出系統架構運用於國軍內部網路，同時配合現行資訊安全通報機制、防火牆與入侵偵測系統，做全方位的「軟硬兼施」組合，希望透過本文提出之架構，使其成為兼具理論與實用之入侵偵測系統，以提供後續研究者參考依據。

收件：97年4月2日
接受：97年4月11日

表二　本系統與Autonomous Agent及AAFID系統功能比較表

功能＼系統	本系統	Autonomous Agent	AAFID
自主性	◎	◎	◎
協同合作	◎	◎	◎
降低網路負荷	◎	◎	◎
溝通能力	◎	◎	◎
離線運作	◎	◎	◎
判斷能力	◎	▲	◎
推理能力	◎	▲	▲
學習性	◎	▲	▲
架構變更	◎	▲	X
即時更新性	◎	◎	▲

◎：擁有全部功能 ▲：擁有部分功能 X：不具備此功能

資料來源：作者綜整