國立交通大學

資訊管理研究所

碩士論文

一個針對無基礎行動網路的聯合防禦式的

入侵偵測機制

A Union-Defense-Based Intrusion Detection

Mechanism for Ad Hoc Networks

研究生：顧吉宇

指導教授：羅濟群教授

中華民國 九十三 年 六 月

一個針對無基礎行動網路的聯合防禦式的入侵偵測機制

A Union-Defense-Based Intrusion Detection Mechanism for Ad Hoc Networks

研 究 生：顧 吉 宇　　Student： Joy Ku

指導教授：羅 濟 群　　Advisor： Chi-Chun Lo

國立交通大學

資訊管理研究所

碩士論文

A Thesis
Submitted to Institute of Information Management
College of Management
National Chiao Tung University
In Partial Fulfillment of the Requirements
For the Degree of
Master of Business Administration
in
Information Management
June 2003
Hsinchu, Taiwan, the Republic of China

中華民國九十二年六月

一個針對無基礎行動網路的聯合防禦式的入侵偵測機制

研究生：顧吉宇　　指導教授：羅濟群 老師

國立交通大學資訊管理研究所

摘要

無基礎行動網路，是一種由少數無線裝置針對特定目的而組成的暫時性網路，具有高度機動性與不須設置硬體設備的優點。無基礎行動網路由於訊號在空氣中傳播，資料安全性與保密性也受到考驗。如何改善資料安全與防範受到入侵攻擊，是目前重要且急需解決的問題。維護網路安全有賴於相互認證和加密方法，與有效的入侵偵測與反饋機制。

本論文針對無基礎行動網路的動態拓樸特性與入侵防禦需求，提出一個聯合防禦式的入侵偵測機制。另於系統實作部分以分散式入侵偵測架構為基礎，整合入侵反應，藉由訊息傳遞達成聯合防禦機制。本論文所提出之機制，經由實驗與實作證明，將使無基礎行動網路可預防各種已知的入侵攻擊與 DoS 攻擊，增加網路本身的安全性與穩定性。

關鍵字: 無線網路，無基礎行動網路，資訊安全，入侵偵測，分散式入侵偵測

A Union-Defense-Based Intrusion Detection Mechanism for Ad Hoc Networks

Student：Joy Ku　　Advisor：Dr. Chi-Chun Lo

Institute of Information Management

Nation Chiao Tung Universite

Abstract

Mobile Ad Hoc Network (MANET), an independent transmission mode, is a temporary network that is composed by wireless device for targeted destination. It provides high mobility and advantage of operating without hardware deployment. Network security relies on authentication and encryption methods between ad hoc nodes，and efficient intrusion detections and response mechanisms.

In this research, we propose a union-defense-based intrusion detection mechanism for ad hoc networks. The system implementation is based on distributed intrusion system with intrusion response, message exchange, and union defense scheme to enhance network security and system stability and protect MANET from malice attack and DoS attack.

Keywords: Mobile ad hoc network，Wireless network，Intrusion detection，Intrusion response，union defense

誌謝

能順利地自交通大學資管所畢業，首先感謝指導教授羅濟群老師，兩年間從羅老師身上學到許多做事的觀念與原則，培養了好的習慣，正如游伯龍老師所說，這些是受用一輩子的寶貝。也感謝口試委員楊千老師與楊建民老師，仔細地閱讀這份論文並給予我寶貴的建議與指點，給了我新的想法與思考方向，沒有老師的指導，就沒有這份論文，在此表達由衷的感謝之意。

還有資管所內一起相處的同學、朋友，從課堂內的互相切搓，課外活動，及許多生活經驗的交流與分享，大大地充實了研究生活的內涵與意義，謝謝你們，這是段充滿美好回憶的日子。

最後感謝陪伴我的父母與妹妹，還有女友瓊茹，讓我感受到溫暖與關懷，謝謝你們的支持與鼓勵。

顧吉宇
交大資管
2004/06/27

目次

圖目次

表目次

第一章　緒論

1.1 研究背景與動機

網路安全的目的，在於確保網路上的資訊安全與電腦安全。從資料完整性，保密性，系統穩定度，遭受攻擊的存活度等議題，可分為許多不同領域。從一次入侵攻擊的時間點來看，剛好可將網路安全分為四個部分，事前：資訊驗證；事發：入侵偵測；事後：資訊存活；事終：資料鑑識。

目前已有相當多研究投入屬於網路安全第一線的事前預防，包括加密，使用者認證，認證中心等機制。面對系統不斷演進，更新，與攻擊型態隨著衍生出複雜，多樣化的手法，單靠預防難以完全防堵。因此屬於第二線的入侵偵測，重要性便日趨提昇。

入侵偵測系統經過了二十幾年的發展與演進，架構日趨複雜，由主機偵測(HIDS)，網路偵測(NIDS)，演變為分散型偵測(Distributed-IDS)。功能也不斷增加，除了入侵偵測，還加入動態分析，誘捕，自動反應，追蹤入侵點等機制，大大地增進了入侵偵測系統的有效性與實務上可行性。

各種不同架構與功能的入侵偵測系統中，都各有其適用狀況與優缺點存在。以分散式入侵偵測系統為例，多點偵測動態分析入侵者的行為模式與特性，找出潛在的危險行為，需花費較多系統資源與時間，運作效率上可能不盡理想；又如適用於有線網路的入侵偵測系統，移植到無線網路時，因無線裝置的網路速度較慢，運算速度較低及網路拓樸型態不同，容易造成偵測效果不彰等問題。

因此針對不同的網路型態與架構，透過研究分析，找出適用於無基礎行動網路之動態拓墣特性的入侵偵測系統，才能有效地提升網路安全，增進系統穩定與存活度，是為本論文發起之動機。

1.2 研究目的

在本論文中，針對無基礎行動網路(Ad Hoc Network)。討論其特殊網路型態，與系統安全性問題，嘗試找出一個適合的動態架構入侵偵測系統。

無基礎網路本身特性，無線網路，多階性，動態拓樸，不可信賴的通訊通道。由於動態拓樸，網路沒有固定節點，每個節點可自由出入網路，使得集中分析，集中管理的方法不適用於無基礎行動網路。其次，當節點間移動迅速時，身份認證方法很容易造成極大的系統負擔，且由於身分認證機制在於確認雙方彼此的身份，若是攻擊者並非以入侵系統為目標，而是另一種型態的攻擊行為。因為入侵系統與癱瘓系統所需花的時間與精力相差極大，例如藉由送大量封包造成該系統無法正常提供服務的攻擊方式，就可能造成網路無法運作。因此，就認證機制而言，無法抵擋這種攻擊，且本身亦受到此種攻擊，而無法提供認證服務。尤其在無基礎行動網路的環境，如何有效的抵擋此種攻擊顯得更為重要。因此，本論文將針對安全性問題進一步探討，如何建立適合無基礎行動網路網路的防禦機制與遭受入侵時的應對方法，藉由聯合防禦的機制提高網路安全與系統穩定度。

1.3 章節規劃

本篇論文目的在於，研究一個在無基礎行動網路上，可實際運作的入侵偵測防禦系統；第二章將探討無基礎行動網路的特性，與無基礎行動網路容易遭受的攻擊類型。接著介紹入侵偵測系統的發展與分散式入侵偵測系統架構，最後討論入侵反應機制的概念與方法； 第三章說明本篇論文所採用的改良方法與系統架構； 在第四章介紹系統實作的模型與實驗數據，效能分析； 第五章則對本系統未來可研究的方向加以討論。

第二章　文獻探討

本章將探討無基礎行動網路的特性，無基礎行動網路的安全問題。接著介紹入侵偵測系統的發展與現行入侵偵測系統架構，最後說明入侵反應機制的概念與方法。以下將分別在各個章節中一一詳述。

2.1 無基礎行動網路

隨著網路環境不斷的改善，各式的通訊服務，如語音、檔、影像得以在上面傳輸。其中以無線網路因它具有可移動性特性，使得它更加受人愛戴。目前無線通訊可分成兩種，一是有基礎架構(infrastructure)之通訊網路環境，例如具有存取點無線區域網路；及無基礎架構之通訊網路環境，即是無基礎行動網路(Mobile Ad Hoc Network，MANET)。由於在有基礎架構之通訊環境須倚賴基地台的存在方能完成細胞(cell)間的轉送。因此，若有基地台損毀、或因自然災害或因基地台電波無法涵蓋的範圍，則此通訊管道失去作用，無線裝置(mobile device)彼此間則無法通訊。而無基礎架構之無基礎行動網路，正可解決上述問題。[6][8]

無基礎行動網路特性即是行動機間之通訊並不須預存一個基礎網路如基地台的設置，它們彼此間能自我組成(Self-Organization)完成構連，建立起通訊管道，而當兩個行動機間已超過無線電電波範圍(radio range)，則另一個行動機即具有路由功能，以搭起此兩通訊機間通訊通道。因此，它除了具有傳統無線通訊的可移動性優點外，又因它具有無基礎架構的特性，其應用範圍更廣，例如，災難救助、軍方作戰演訓、辦公室會議環境及航空運用。

2.1.1 無基礎行動網路的運作方式

無基礎行動網路是一種獨立型的基本服務組合(Independent Basic Service Set)[11]。在 IBSS 中，行動機彼此之前可以直接通訊，兩者的距離必須在可以直接通訊的範圍內。以 802.11 所提供的 Ad hoc 模式而言，最低限度的網路，是由兩台行動機組成的基本服務組合，通常是由少數幾部行動機針對特定目的而組成的暫時性網路。常見的情況是在會議室中支援個別會議之用。會議一開始與會人員彼此會形成一個無基礎行動網路以便傳輸資料。當會議結束時，網路隨即瓦解。正因為持續時間不長，規模甚小且目的特殊，無基礎行動網路也被稱為特設服務組合(Ad Hoc BSS) 或特設網路(Ad Hoc Network)，由於此種網路的點對點(peer-to-peer)性質，有時亦稱為點對點網路。網路示意圖如下:

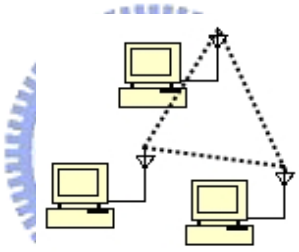

圖 2-1　無基礎行動網路示意圖

2.1.2 無基礎行動網路的安全議題

標準的無線網路，無線裝置透過基地台(Access Point)與網路上其他設備，如路由器，閘道器，名稱伺服器等裝置互相通訊。相對的，無基礎行動網路沒有固定裝置，無線裝置可能發生錯誤而造成網路失效。缺乏固定裝置而造成難以認證的問題，使得傳統認證機制無法使用，無法辨認無線裝置是否可信賴，讓整個網路暴露在遭受攻擊的危險中。

無基礎行動網路還潛在另一個問題，由於路由資訊是每個參與網路的節點所共同協調組成，傳遞資訊。當系統難以辨認無線裝置是否可信賴時，若組成網路的節點其中之一進行惡意行為，包括散佈錯誤路由訊息，竊取資訊，很難被辨認出

來，造成網路通訊的安全問題。

目前大部分研究均投入動態拓樸及服務品質上的問題探討，就不可信任的網路環境，所引起的安全性問題討論較少；而在無基礎行動網路環境下討論安全機制問題，其原因包括：

1. 無線網路本身即是一個受攻擊的通訊環境，不管是竊聽、幹擾或是阻斷服務的攻擊，都會造成嚴重的影響。
2. 長時間通訊下一些非法入侵的行為是不可避免的。
3. 無基礎行動網路它是一種無基礎架構的網路環境，因此並未具有集中式管理的特性。
4. 通訊機隨時可能加入或移出某一個通訊區域。

從上述問題得知，在此無線通訊環境中應具有身份驗證(Authentication)、私密性(Confidentiality)、資料傳遞的正確性(Integrity)、不可否認性(Non-repudiation)及存取控制(Access control)等機制，提高網路安全性與可信賴性。做為發展無基礎行動網路相關應用的基礎。

2.1.3 無基礎行動網路常見的入侵攻擊

除了基本認證機制做為網路安全的第一道防線，面臨惡意入侵與攻擊時，由於無基礎行動網路架構上的弱點，造成的攻擊問題包括：

1. 黑洞問題(Black hole)

被入侵的節點利用無基礎行動網路路由協定發送假冒的路由資料，使其他節點對於最短路徑的判斷錯誤，將資訊送到錯誤的路徑而無法正確傳輸。

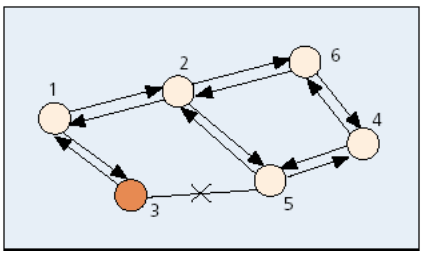

圖 2-2　黑洞問題示意圖

2. 阻斷式服務攻擊(Denial of service)

攻擊者由外部網路或被入侵的結點，發送大量控制訊息封包，使得頻寬被佔據而無法傳送資料。

3. 溢滿式路由攻擊(Routing table overflow)

被入侵的節點藉由偽造的路由資訊，使欲攻擊的節點誤以為有另外一條路徑存在，而將資料送往不正確的路徑。

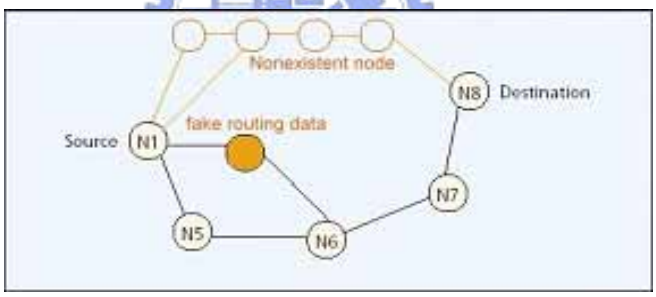

圖 2-3　溢滿式路由攻擊示意圖

4. 仿冒節點問題(Impersonation)

一個惡意節點偽造假的控制封包，更新附近節點的路由資訊，使得原本應該傳給某個特定節點的資訊，轉送到惡意節點。用以竊取某些特定資訊。

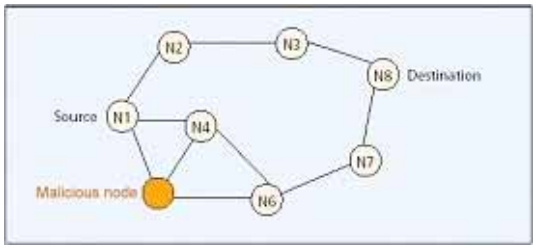

圖 2-4　仿冒節點問題示意圖

5. 消耗電力問題(Energy consummation)

惡意節點持續送出需要傳送到網路另一端的無意義資料，使得附近的節點無法進入睡眠模式，持續轉送資料，消耗無線裝置的電力。

6. 資訊外流問題(Information disclosure)

無基礎行動網路需要藉著其他節點協助進行資料傳遞。因此中繼節點可截取傳輸的資訊，若傳送者與接收者中間必須透過某些未被身分認證的節點傳送時，資訊即有可能外流而造成傷害。

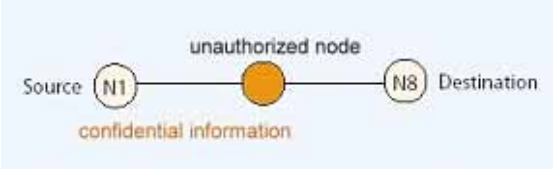

圖 2-5　資訊外流問題

基於上述所提無基礎行動網路架構而衍生的相關安全性問題，本論文將針對入侵發生時的即時偵測應對機制做更進一步探討，以期提出一個在無基礎行動網路上對於安全問題的解決方案。

2.2 入侵偵測系統的發展與演進

入侵偵測系統發展至今已超過 20 年，最早出現入侵偵測概念起源於 1980 年 James. P. Anderson 所提出一篇名為「Computer Security Threat Monitoring and Surveillance」的文章。裡面提出審查與監視(Monitoring)的觀念，對電腦系統進行監督，由系統記錄與安全記錄中分析資料與辨識異常資訊，發掘安全性問題，藉以保護系統安全。

入侵偵測系統的基本運作方式由兩個部分組成:

1. 資料收集方式

決定入侵偵測系統所偵測的目標與安全監督的重點，可分為主機型(Host-Based)與網路型(Network-Based)。

2. 偵測方式

如何對收集的資料進行偵測與比對，找出問題點，可分為異常檢測型(Anomaly)與誤用型(Misuse)。資料收集方式與偵測方式間的對應關係可由下表中得知，共有四種不同類型的入侵偵測系統，並列出早期出現的相關研究。

表 2-1　資料收集與偵測方式對應表

		資料收集方式	
		主機型	網路型
偵測方式	異常檢測型	A	C
	誤用型	B	D

A. 於 1980 年提出的「Computer Security Threat Monitoring and Surveillance」是為最早的入侵偵測系統概念

B. 1984 年開始發展的 IDES(Intrusion Detection Expert System)，第一個實作出來的即時入侵偵測模型，結合統計模型與專家系統作為偵測技術。

C. 1990 年 NSM(Network Security Monitor)，最早提出以網路封包作為資料來源的入侵偵測系統。

D. 1990 年提出的「A Unix Prototype for Intrusion and Anomaly Detection in Secure Networks」[3]，結合網路型與誤用型偵測，由封包資料分析系統運作時正常與異常狀態的方法。

2.2.1 資料收集方式

此後到 1990 年間，出現許多入侵偵測方線的相關研究，以架構來看，主要有兩種類型的入侵偵測系統在此時期奠定基礎。

- 主機型入侵偵測系統(Host-Based IDS)

主機型入侵偵測系統的運作方式為，監視系統的運作紀錄，找出可疑的攻擊行為，並發出警告通知管理人員。主機型入侵偵測除了可以追蹤重要的系統記錄外，也可以定期對重要的系統檔案進行檢查，以確保檔案沒有受到惡意的入侵或修改。

- 網路型入侵偵測系統(Network-Based IDS)

網路型入侵偵測系統是以蒐集在網路上流通的封包，作為判斷網路或者主機是否遭受攻擊者的攻擊或者入侵的依據。而且因為網路上的溝通必須遵守共通的通訊協定，所以產生的封包格式必須具有一定的規格，而這些封包在格式上並不會因為所用的電腦平臺不同，或者是作業系統的不同而有所差異。網路型入侵偵測系統，必須建構在其所保護的內部網路上，也就是說整個存在其內部的網路中的網路資料溝通必須透過它的檢查。而且由於它並不是利用主機上的紀錄資訊作為其判斷是否主機被入侵的資料，所以它所保護的內部網路內的電腦可以是任何一種平臺，或是任何一種作業系統。所以在應用上有更大的彈性而不受平臺及作業系統的束縛。如下圖所示，網路型入侵偵測系統架構圖

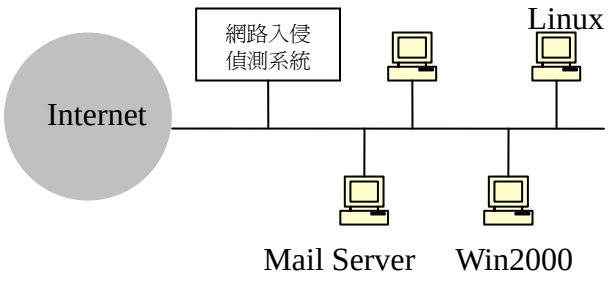

圖 2-6　網路型入侵偵測系統架構圖

網路型入侵偵測系統，因為它監測的是所有電腦共通的封包，所以偵測系統與被監測的對象之間，不需要特定是哪一種平臺或作業。但是也正因為如此，假若是針對特定一種作業系統，或特定型態的主機所發動的入侵攻擊行為，這種以網路為主的入侵偵測系統的抵禦能力，在這時候就明顯的不如單純保護主機的入侵偵測系統完整周密。

2.2.2 偵測方式

將入侵偵測系統依照偵測方式的不同分類，可分為：異常檢測型(Anomaly IDS)和誤用檢測型(Misuse IDS)。異常檢測型入侵偵測系統的概念是: 先記錄系統平時正常運作的狀態，將資料分類歸檔記錄，定義為所謂的「正常狀態」。偵測時將讀取的資料與系統正常狀態進行比對，若發現不吻合的情況，便判定為異常行為，此為系統運作之目的，將不屬於正常狀態中的行為經由分析比對找到異常狀態。反之，先將系統各種異常行為記錄，找出特徵後，進行比對找出特定異常行為的系統，便稱為誤用檢測型系統。

兩種系統最主要的差異，由於異常檢測型是依據預先定義的正常狀態進行偵測與分析，當正常狀態定義得不夠詳細與完整時，系統誤判率非常高，所有未被定義的行為都會被當成異常。反之，誤用偵測型是仰賴預先定義的錯誤情況，藉以判斷是否符合錯誤。當錯誤狀況定義不夠完整時，系統的偵測能力便會大受影響。此外，當異常行為定義增加時，也容易造成系統比對上的負擔。

2.2.3 分散式入侵偵測系統

分散式入侵偵測系統(DIDS)[17]最早出現於1990年，由美國加州大學Davis分校(UC Davis)提出，其主要目的為追蹤使用者在網路內的移動，利用賦予使用

者一個獨特的辨識碼(NID)來追蹤使用者的行為。

入侵偵測系統的發展由分散式入侵偵測開始，架構由單一電腦，轉變為多台電腦分析，優點是涵蓋不同網域，得到更多資料提供偵測分析，可藉此判斷更複雜的攻擊行為。進入分散架構延伸出來的問題，包括整體規劃，系統間的協調機制，管理方式，攻擊分析，偵測效率等，也成為入侵偵測系統近十年來的熱門研究課題。

分散式入侵偵測系統結合了主機型與網路型系統的特點，能自不同的主機或網段收集資料，並分析不同資料來源間的關係、偵測對主機或網段的入侵行為，辨別入侵行為之間的關聯性。如圖 2-7 所示，分散式入侵系統之架構示意圖

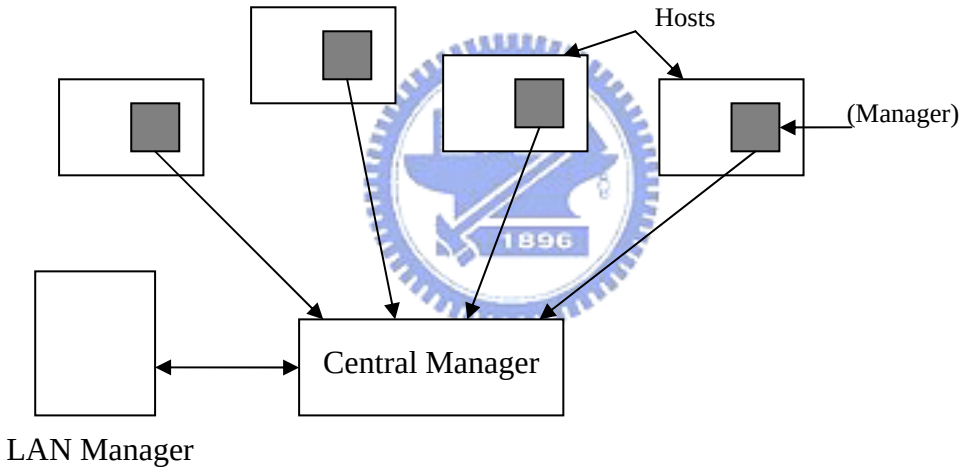

圖 2-7　分散式入侵偵測系統架構

依照陳亦明教授發表於 2002 年資訊安全期刊對於分散式入侵偵測系統的整理[18]，其中對於分散式入侵偵測系統的定義為:『為一入侵偵測系統，能自不同的主機或網段收集資訊，綜合分析這些不同資料來源的資訊間的關係，以偵測橫跨於不同主機或網段的入侵行為，或找出個別發生於不同主機或網段的入侵行為間的關係。』

目前已有許多關於分散式入侵偵測系統的研究。茲將一些較為著名的研究列出如下：

- DIDS (Distributed Intrusion Detection System)

  DIDS[17]主要包括數個 LAN Monitor 與數個 Host Monitor 分別蒐集網路封包與主機紀錄，然後將相關資訊送往 DIDS Director 進行分析。

- GrIDS (Graph-based Intrusion Detection System)

  GrIDS[16]其目的在於偵測如 Worm、 DoS 等分散式入侵行為。GrIDS 將觀察到的入侵行為以活動圖的方式表現，利用階層式架構與使用者定義的規則，合併相關的活動圖。若活動圖合併後大小超過預定 Threshold，則可能發生了大規模的入侵事件。

- Prelude-IDS

  Prelude-IDS[5]多階層入侵偵測系統，特色在於處理功能皆經過模組化，可抽離或增加組成大型偵測系統，後端產生的分析資料可轉為使用者指定的標準格式，如 SQL 資料、 XML 等，用以作為進一步分析與判斷的依據。

- EMERALD (Event Monitoring Enabling Response to anomalous Live Disturbances)

  EMERALD[14]一套具有可擴充性的分散式入侵偵測架構，以整合各類資訊安全系統。系統主要由許多 Monitor 組成，透過階層式架構加以組織協調。EMERALD 強調的重點是對於異質性系統的整合能力，而非建立關係緊密，分工細緻的系統。因此對於關聯性分析，偵測分散式入侵的能力也較為缺乏。

- AAFID (Autonomous Agents for Intrusion Detection)

  AAFID[2]主要目的在建立一套具有可擴充性的分散式入侵偵測系統。該系統採用階層式架構，使用自治代理人的技術，代理人用來執行特定用途的程式，如監控主機的連線數量，或偵測特定格式的入侵行為，然而代理人不能互相溝通，必須透過上層的協調單元傳送資料。

- MAIDS (Mobile Agents for Intrusion Detection System)

  MAIDS[9]分散式分析的入侵偵測系統，由許多單一功能的代理人程式共同組成。系統利用 Software Fault Tree(SFT)與 Colored Petri Net(CPN)描述分散式攻擊行為，其分析結果能直接對應到所需的代理人程式，利用 SFT 建立入侵行為模型，再進一步描述信任關係、時間性關係與前後關係，以修正入侵行為模型，增加準確度。

- CARDS

CARDS[4]目的在建構一套非集中式的入侵偵測系統，主要用特徵比對找出入侵行為，系統間利用分解後的特徵產生 System views，藉此找出事件間的相依關係，偵測分散式入侵行為。

從上面的整理中，綜觀目前發展的分散式入侵偵測系統，著重在關聯性分析，增加系統偵測複雜入侵型式的能力。以集中式或分散式架構為主，掃描多個資料來源，將資料整合處理，傳給中央的主控台分析不同資料間的關聯，及資訊比對與提供使用者驗證資料的介面。重點在於找出，複雜類型的入侵與異常，增加偵測效率。而無基礎行動網路動態網路拓樸，需要具有分散管理，機動式協調特性的入侵偵測系統才可符合需求。應用在無基礎行動網路上，當負責收集、檢索入侵資訊的主控台若登出網路，要如何交換資訊給下一個主控台，若主控台無預警的登出，其他的節點是否可快速的產生另一個主控台等問題，這些相關課題目前仍沒有定論。

分散分析式系統屬於分散式系統的延伸，消除偵測系統間的階層式關係，或可容許短暫的缺乏管理機制。系統間自動分工合作，仰賴有效的溝通聯絡機制，此類系統特性在於每個節點的入侵偵測系統之間都是相同的，沒有主從之分，同時包含掃描與分析功能。系統之間必須有適當的訊息傳遞與資訊溝通，才能讓其他節點將資訊整合起來，進行分析動作。

目前發展中的系統架構，對於訊息傳遞的安全機制較少被提及，包含如何在不安全與不可信賴的網路架構上傳送訊息。在大規模的網路攻擊中，入侵偵測有可能被當作攻擊對象之一，特別是安全防護較弱的無線網路，資料篡改與偽造特別容易。這也是相關研究需要深入探討的部份。分散分析式入侵偵測系統示意圖如圖 2-8:

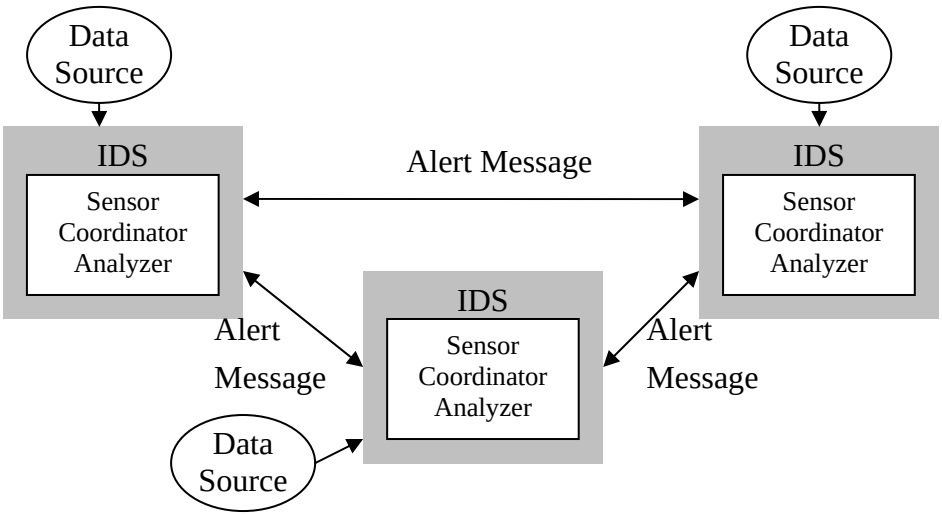

圖 2-8　分散分析式入侵偵測系統架構

此外，正由 IDWG 提交 IESG 審核中的入侵偵測訊息交換格式(IDMEF)[1]，是針對異質入侵偵測而發展出來的標準。IDMEF 的目標在制定一個入侵偵測系統間傳遞訊息公開的資料格式標準，讓入侵偵測系統可以分析，發現可能攻擊行為，將警告訊息傳遞給其他入侵偵測系統或上層的管理系統。警告訊息包括回報可疑事件，可能發生的攻擊行為，確認攻擊者的來源，受攻擊的範圍與應用程式，使不同系統間可以透過統一格式，瞭解運用這些訊息。目前 IDMEF 是以 XML 格式描述定義。

2.3 入侵反應系統 (IRS)

傳統入侵偵測研究主要針對偵測方式進行改良，目的在於提升偵測準確度，效率與多型態的偵測方式。對於偵測攻擊的後續反應，交給系統管理者決定，系統本身不具評估與判斷能力。面對目標明確的入侵方式，如溢位元攻擊，後門攻擊，的確需要人為判斷與處理。然而隨著安全認證與加密機制日漸嚴密，傳統攻擊逐漸減少，攻擊方式也轉換為半自動或自動的方式，攻擊者只需要啟動一次攻擊，程式便會自動複製與散佈，入侵其他網路上的裝置，令傳統的防禦機制無法負荷，防不勝防，無法單純仰賴人為處理。如阻斷式攻擊(DoS)，蠕蟲病毒(Worm)，

或 Email 散佈等方式。入侵反應系統的存在便顯得日漸重要。

入侵反應系統類型可分為三種方式

1. 提醒 (Notification)

   將入侵偵測系統發出的警告加入記錄，並主動通知管理者。

2. 手動反應 (Manual Response)

   將反制入侵的方法預先寫好程式，讓管理者決定採用何種反應方式。如控制防火牆阻擋，或將被攻擊的電腦關機等方式。

3. 自動反應 (Autonomous Response)

   系統依照偵測系統所發出的警告，自動判斷與進行系統防禦動作，不需透過人為介入，管理者可透過修改自動判斷的規則，達到安全防護的效果。

入侵反應系統目的在於處理入侵偵測系統發現問題之後的後續動作。由網路安全觀點，偵測系統是偵測異常行為，入侵反應則是針對異常行為做出反制動作。藉由兩個系統協調運作才是完整的系統防護機制。

2.3.1 調適型入侵反應系統(Adaptation in Intrusion Response)

調適型入侵反應系統較完整的架構於 2000 年提出「Adaptation techniques for intrusion detection and intrusion response systems」[15]。其系統架構圖如下:

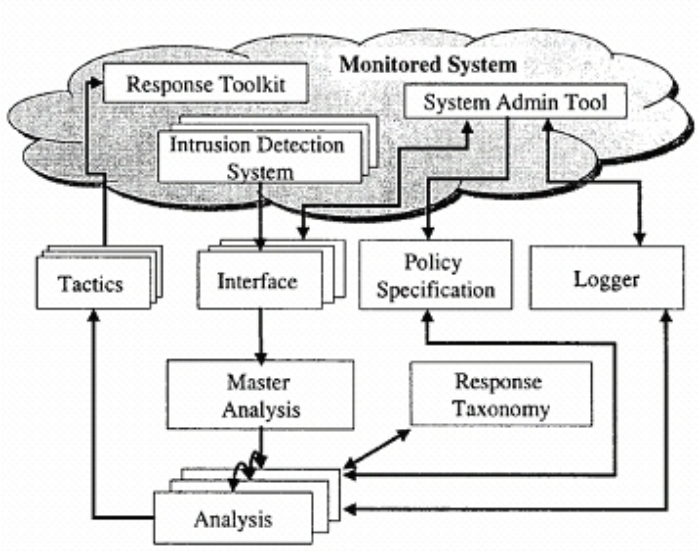

圖 2-9　調適型入侵偵測與反應系統

系統概念為，根據入侵偵測系統所發出的警告，後端回應介面(Interface)接收之後，交給主分析元件判斷(Master Analysis)。主分析元件將警告轉發給分析元件(Analysis)，根據歷史紀錄決定警告的可信賴度，當確認此警告是可信賴之後，經過回應分類元件(Response Taxonomy)決定屬於何種回應方式，交給策略元件(Tactics)決定該如何回應本次的攻擊行為，最後透過回應元件(Response Toolkit)做出反應。

舉例說明，當系統受到入侵攻擊時，同時有兩個偵測器 A，B 發出警告，系統經由主分析元件判斷，決定偵測器 A 的信賴度較高，便以偵測器 A 所收集的資訊作為回應依據。交由策略元件執行防禦策略，透過回應元件通知外圍的防火牆對此攻擊來源 IP 進行過濾動作，將有問題的封包阻絕於系統之外。

由適應型系統架構中可以看出，當入侵偵測系統發出警告後，入侵反應共分有三個階段需要系統進行評估判斷。

1. 判斷警告是否可信賴
2. 依照警告類型是否回應或防禦
3. 採取何種防禦策略最為有效

在上述階段，需要依照系統運作的情況判斷與自我審核的機制，自動調適回應策略，才能達到最佳化防禦的效果。

2.3.2 聯合防禦(Union Defense)

在上一節中我們討論了入侵反應的概念，這節將繼續探討如何將入侵反應與防禦策略連接在一起，進而實際達到維護網路安全的成果。

在今日的網路攻擊模式下，網路防禦的目標應是雙面的； 除了防止被攻擊外，也要避免網路內部的主機成為攻擊跳板。利用網路型偵測系統，探查 ICMP，UDP，TCP 的封包內容，比對有危險性的封包以找出攻擊來源，如此就能過濾掉許多的攻擊行為。本章節將探討區域網路之防禦方式，架構設計與安全議題。

聯合防禦概念(Union Defense)起源於黃能富教授於 2002 年發表在 TANET 的一篇論文[12]，提出一個實作的區域聯防架構。目的在於建立一個安全的網路聯防系統，藉以提升網路防護能力。架構圖如下所示。

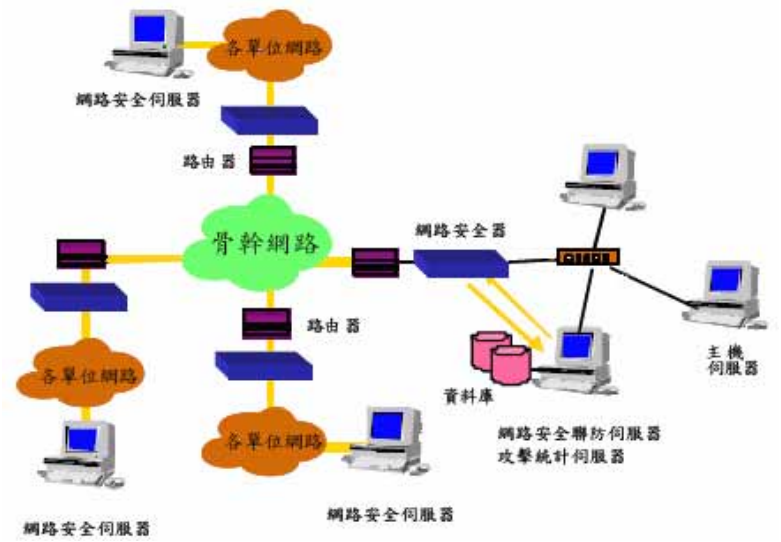

圖 2-10　區域網路聯合防禦架構

在網路聯合防禦架構中，共分為四個主要元件，分別說明如下

1. 網路安全器 – 網路安全系統的實體主機。位於對外路由器以及代管網域之間，所有流量必經之地，它負責檢查所有經過之封包。並於偵測出網路攻擊後立即將該攻擊之封包攔截並丟棄，始知不影響網路之電腦。同時也將網路攻擊紀錄以及網路安全器所歷經之事件回報給網路安全政策伺服器。

2. 網路安全政策制定介面 – 提供網路安全管理之政策制定介面，管理者可以經由此介面方便制定網路安全之管理方式。

3. 網路安全政策伺服器 – 網物安全政策伺服器「網路安全器」是及「網路安全政策制定介面」溝通的橋樑。此外它也負責記錄索有網路安全器所產生的警告訊息。

4. 統計報表系統 – 內建於政策伺服器。藉由與網路安全氣溝通以提供網管人員更多統計資訊，藉以判斷整體網路狀況與入侵訊息。

每個需要防禦的區域網路皆裝置一台「網路安全器」，與「網路安全伺服器」，平時可以執行各區域網路的自行制訂的安全政策。同時也配合整體網路有一套聯防控制系統。透過聯防機制與聯防政策，共同防護網路安全。

舉例說明，當分散式阻斷攻擊發動時，往往是經由多台電腦同時對目標網域進行攻擊，因此藉由單一的網路安全器可能面臨同樣被攻擊癱瘓的問題。當攻擊對聯合防禦的網路發動時，網路安全伺服器與網路安全器透過聯防系統共同運作，當某台網路安全器偵測出入侵行為，立即通知其他網路安全器一起協同阻擋，便能同時分擔攻擊的效果，將攻擊阻絕於整個網路之外。

聯合防禦架構對於癱瘓系統類型的攻擊特別具有防禦效果，網路安全器所能承載的網路流量與系統效能遠大於單一電腦主機。因此由許多台網路安全器共同承受攻擊，更能有效分擔運算成本，讓網路保持安全穩定的狀態.

第三章　聯合防禦式的入侵偵測系統

本章主要討論運作於無基礎行動網路的入侵偵測系統有哪些需求，與系統設計之考量，規劃偵測模組間溝通與協調方式，並藉由聯合防禦機制，以達到系統安全之目的。另依據先前所提之分散分析式架構進行修改，實作一個運用於無基礎行動網路環境下聯合防禦式的入侵偵測系統。

3.1 建構於無基礎行動網路的入侵偵測系統需求

無基礎行動網路因為沒有固定裝置支援，完全由各行動機互相傳遞資料，連結成為一個動態網路架構，網路的每一個節點都參與資料通訊的過程。特色是不需要事先設置固定式裝置，如基地台，集線器裝置即可互相通訊，設置成本低廉，擁有極佳的便利性，透過無線傳輸不需受到環境地形限制。其特色也是發展於無基礎行動網路的應用系統所面臨最大挑戰，由於其動態架構，固定式的網路概念無法適用於此特殊型態的網路，以下我們便根據文獻探討中所提的無基礎行動網路特性[7]，分析其所需的入侵偵測系統需求:

表 3-1　無基礎行動網路與入侵偵測設計分析表

無基礎行動網路特性	入侵偵測系統面臨的問題
沒有固定裝置可提供權責控管或集中管理的功能	無法採取階層式或集中式管理系統架構，傳統的分散式入侵偵測系統架構，採取由中控伺服器負責收集與分析記錄，並通知使用者。此種方式便無法適用於無基礎行動網路。此外，如何處理節點間的溝通與運作，提高偵測效率也是一重要課題。

網路拓樸動態改變	節點的移入移出可能相當迅速，也不會固定在網路中的某個位置，因此當網路中有某個節點加入或離開時，系統需要不受影響地持續運作，保持整體入侵偵測防護機制正常。
無線裝置本身也負責路由傳遞	節點本身也有可能成為攻擊來源，或入侵攻擊的跳板，因此防禦機制中，需有排除內部網路有問題節點的技術，與偵測方式。
無線裝置的能源供給有限	由於無線裝置所能使用的電力有限，面對消耗性和癱瘓系統的攻擊方式，需有快速有效的應對方法。

從上表分析可以發現，傳統只仰賴單一節點進行偵測的主機型或網路型入侵偵測系統，收集資料來源有限。通訊可能只在某些節點之間進行，而非傳遞於整體網路，收集某一主機的系統資訊，或收集某一節點的網路封包，不足以達到監控整體網路的目標。因此架構方面需朝向分散式系統架構設計，將偵測器佈置於網路中各節點，才能達到完整的監控功能。

其次，入侵反應防禦機制的考量，由固定式網路的觀點出發，固定式的網路防護是由入侵偵測裝置，與防火牆共同組成，偵測裝置發現入侵問題，透過入侵反應元件通知前端防火牆對攻擊來源進行過濾與監視，而達到防護效果。採取此種防禦策略，因為固定式網路架構乃是透過實體的網路線，與路由器，橋接器，防火牆等網路裝置所組成，偵測系統只是網路的子節點，發現入侵行為時，偵測系統本身不具備防護其他電腦裝置的能力，必須透過外圍的防禦裝置執行防禦策略。其架構圖如圖 3-1

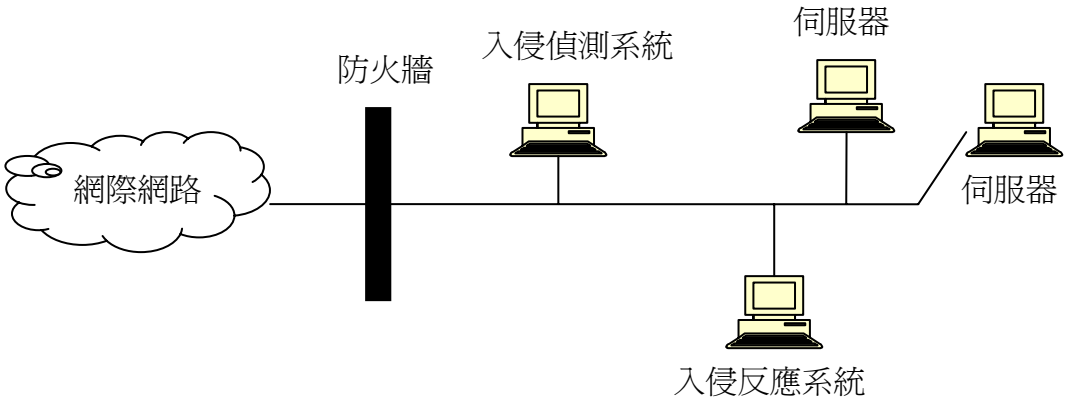

圖 3-1　固定式網路入侵偵測與反應系統

若考慮將入侵偵測或入侵反應系統嵌入防火牆或網路連接裝置，雖然可以針對整個網路達到防護效果，但這些裝置同時需要處理整個區域網路的資料量，本身運作需消耗極大運算效能，容易導致運作效率不佳的問題。

相對而言，無基礎行動網路本身是仰賴節點之間進行路由與資料傳遞，節點本身即為網路設施，負責傳遞資料與建立路由，並沒有如防火牆的裝置可統一過濾網路封包。且資料量與節點數量成正比，所有節點平均分擔整體網路流量，因此若把過濾與阻擋的功能整合於入侵系統本身，防禦機制建構在每個節點上，即時由入侵反應元件啟動防禦策略，即能達到防護效果。異常封包在經過有偵測系統的節點時，會遭受阻擋而不將資料傳給其他節點，進而達到維護整體網路安全之目的。將每個無基礎行動網路的節點包含入侵偵測與反應功能，其示意圖如下圖 3-2，每個節點分別執行入侵偵測與反應。

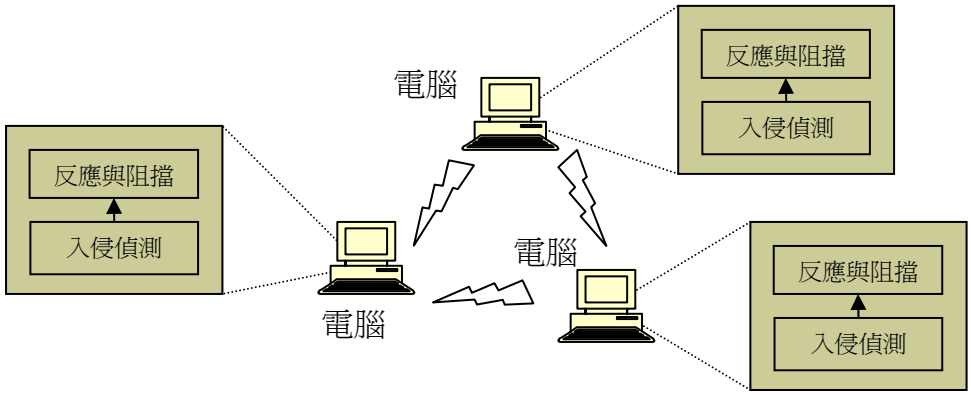

圖 3-2　無基礎行動網路入侵偵測與反應系統

現行的分散式分析入侵偵測系統中，若採取集中管理與階層式管理，或架構中有無法缺少與取代的功能元件的設計，皆不符合無基礎行動網路特性。故需重新考量其架構需求。綜合以上分析，我們可以整理出適用於無基礎行動網路的入侵偵測系統的條件:

1. 單一節點的功能完整，由入侵偵測與反應元件共同組成。
2. 節點間可互相溝通，不需透過另一層的管理協調機制，即可傳遞資訊。
3. 節點本身必須有阻擋功能，配合入侵反應達到整體網路的防護效果。
4. 入侵偵測系統本身不能成為攻擊的目標與安全漏洞。

3.2 聯合防禦式架構

為符合無基礎行動網路特性，在前一節已討論整理得到入侵偵測系統的需求，因此在本節我們依據這些需求，設計與整理一個適用無基礎行動網路的入侵偵測系統架構，就聯合防禦機制進行討論。

架構上採取分散式分析的方法作為入侵偵測系統發展方向，理由已在 3.1 節描述，分散式分析入侵偵測系統的資料來源透過擷取網路上流動的封包進行比對，及早發現異常行為。將入侵偵測系統置於無基礎行動網路節點，隨著節點移動而進行偵測。由於無基礎行動網路的拓樸型態為動態改變，資料傳遞路徑隨著節點的位置不同而修正。原先傳遞異常封包路徑上的節點一旦遭到替換，而異常封包及攻擊行為仍持續出現，則新的節點需要重新開始偵測與反應的程式進行防禦。因此，若節點在偵測到異常狀態後，本身執行防禦阻擋動作，又能通知其他節點共同進行聯合防禦，就能預先將可疑的攻擊阻絕於節點之外，並節省重複偵測的時間。

其次，入侵偵測與入侵反應系統的關係，由單一節點拓展為多點運作時，需

考慮資訊交換的問題。當只有一台主機執行入侵偵測與入侵反應系統時，運作透過內部記憶體交換，資訊交換成本幾近於零，不需考慮運算與傳輸時間的問題。但是當多點運作時，入侵偵測與入侵反應需透過網路傳遞資訊。將節點間的傳輸成本列入計算，便需要從整體網路的流量與傳輸方式重新考量。以交通大學的網路環境為例，每台主機一天約可偵測到 5000-20000 次異常入侵，若每個節點在偵測到異常情況後發出訊息通知其他節點，每個節點送出一次通知，造成的網路流量便十分可觀，對無線網路而言更是極大負擔。進一步地觀察，網路異常行為有輕重緩急之分。篩選較嚴重的警告傳給別的節點，比不分類直接傳遞更能節省資源與效率。因此架構中加入了入侵偵測與反應機制之間的警告分類，過濾較輕微的入侵警告，將嚴重或危急的警告傳遞給其他節點，才能有效地降低影響以避免聯合防禦機制本身成為網路的負擔。聯合偵測防禦的系統架構如圖 3-3:

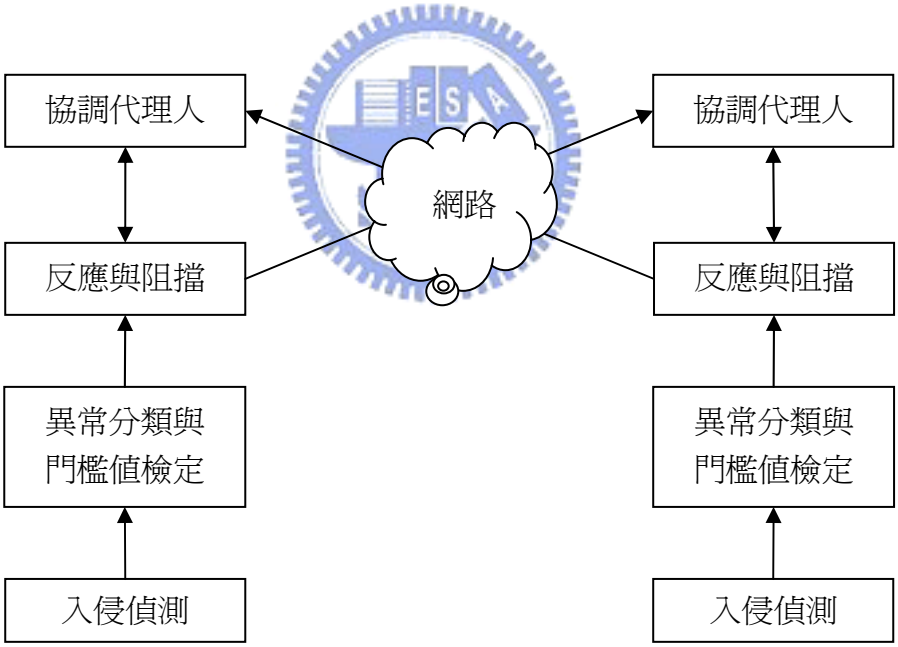

圖 3-3　聯合式的入侵防禦機制

- 入侵偵測

  為網路型入侵偵測，抓取網路封包將封包解析後比對是否為異常類型。

- 異常分類與門檻值檢定

  接收由入侵偵測系統所傳來的警告，由於異常警告視偵測情況而有嚴重程度

之差異，我們將警告分為三大類，其分類表 3-2 如下所示:

表 3-2　異常警告分類

警告類型	系統判斷處理
異常攻擊警告	通知其他入侵偵測系統
普通異常警告	經由門檻值篩選
輕微警告	不處理

最嚴重的攻擊類型警告，由於系統直接遭受攻擊，除了進行防禦策略外，同時通知其他節點，以免網路遭受更嚴重傷害。而普通異常警告主要為網路掃瞄，或主機弱點偵測等情節較輕的異常狀況，雖不會立即對系統造成傷害，但可能在發現網路的弱點之後，發動更危險的攻擊行為，因此我們利用門檻值篩選，從此類別的異常警告，選出較頻繁發生的異常資訊傳遞給其他節點，藉以達成聯合式防禦。門檻值依照網路狀況而定，此部分將在第四章實作階段進行討論。

- 反應與阻擋

當系統接收到經由分類與篩選過的警告之後，執行阻擋防禦，將入侵攻擊來源的封包丟棄，不傳遞給網路的其他節點。

- 協調代理人

負責接收由其他入侵反應系統所傳來的警告訊息。在聯合式的偵測機制中，由於需要透過網路接收訊息，須考慮系統本身是否可能成為攻擊者目標，收到偽造訊息讓入侵偵測系統執行不正確的防禦動作，使網路在傳輸時丟棄錯誤的封包，造成安全性問題。所以本論文中參考" Voting methods for multiple autonomous agents "[13] 所討論的多數決投票方法(Majority Vote) 作為協調模組的決策根據。

(發出警告的節點 / 網路的全部節點) > 0.5

多數決投票的觀念應用於無基礎行動網路，所有的節點都有機會發出是否針對某個入侵來源進行阻擋的警告訊息，考量到可能有偽造警告訊息，不能只接受一個節點的訊息即做出判斷，若發出警告的節點超過網路全部節點的半數，才接受此訊息。假設在最少網路節點數的情況，由兩個節點組成的無基礎行動網路也需要兩個節點都發出通知才會超過半數。因此單一攻擊來源無法偽造訊息讓系統判斷錯誤，能防止入侵偵測機制受不正確的資訊所誤導。此外，多數投票決的方法當網路節點數量改變時，投票結果也會隨之修正，能因應無基礎行動網路節點動態加入或離開的特性，維持正常運作.

3.3 小結

在本章節中，我們依照無基礎行動網路的特性，深入探討系統建構的特殊需求，與安全性議題。根據過去研究所提出的成功概念，與實際運作入侵偵測系統所得到的結論，提出一個具備可行性的入侵偵測系統架構，規劃運作流程與系統模組，以期得到預期的實驗成果。

第四章　系統設計與模擬

4.1 測試平臺與環境說明

本論文之實驗環境架構於交通大學校園網路，由四台電腦依本實驗之特定目的而組成的特設網路，進行以特設網路為基礎的聯合防禦式的入侵偵測機制，其硬體設備與環境狀態列出如下。

(1) 偵測與聯防機制運作節點:

硬體:

CPU: AMD Athlon 1.3G

AMD Athlon 2.5G

Intel Pentium4 2.4G

硬碟空間: 10G Bytes

網路介面卡: 3Com 905C-TX / Realtek 8139 / Realtek 8139

無線網卡: Z-COM XI-626 / Inter(R) PRO, Wireless LAN2100

作業系統:

Window 2000 Professional

(2) 資料庫伺服器:

硬體:

CPU: AMD Athlon 1.3G

硬碟空間: 30G Bytes

網路介面卡: 3Com EtherLink Server 10/100

作業系統:

Window 2000 Advance Server

資料庫:

MySQL 4.0 release

(3) 網路環境:

交通大學校園網路: 乙太網路 10MBps / 100MBps

無線網路: 802.11b

(4) 開發平臺:

Window 2000 server

Visual C++ Version 6

4.2 系統模擬

為求本實驗之實作可行性,系統實作採取開放原始碼架構的 Snort 網路型入侵偵測系統[10]進行修改。Snort 是一套著名的開放原始碼的軟體,由許多人共同參與開發,偵測入侵能力不輸給商業版的入侵偵測系統,且 Snort 的程式碼是公開的,對於需要修改,加入新功能測試模組的實驗十分適合。只要修改程式碼後將自己的程式碼公開提供其他人使用,就沒有智慧財產權相關的法律問題,且公開研究心得對於相關領域的研究相信會有正面幫助。

Snort 是一個異常檢測型網路偵測系統,其運作方式為讀取網路封包,經過封包重組解析的前置處理後,比對現有特徵資料庫,檢查封包是否有異常特徵,若比對得知為不正常的封包,則依照預先設定的延伸處理方式,將警告儲存或發出提醒。其系統流程圖如下:

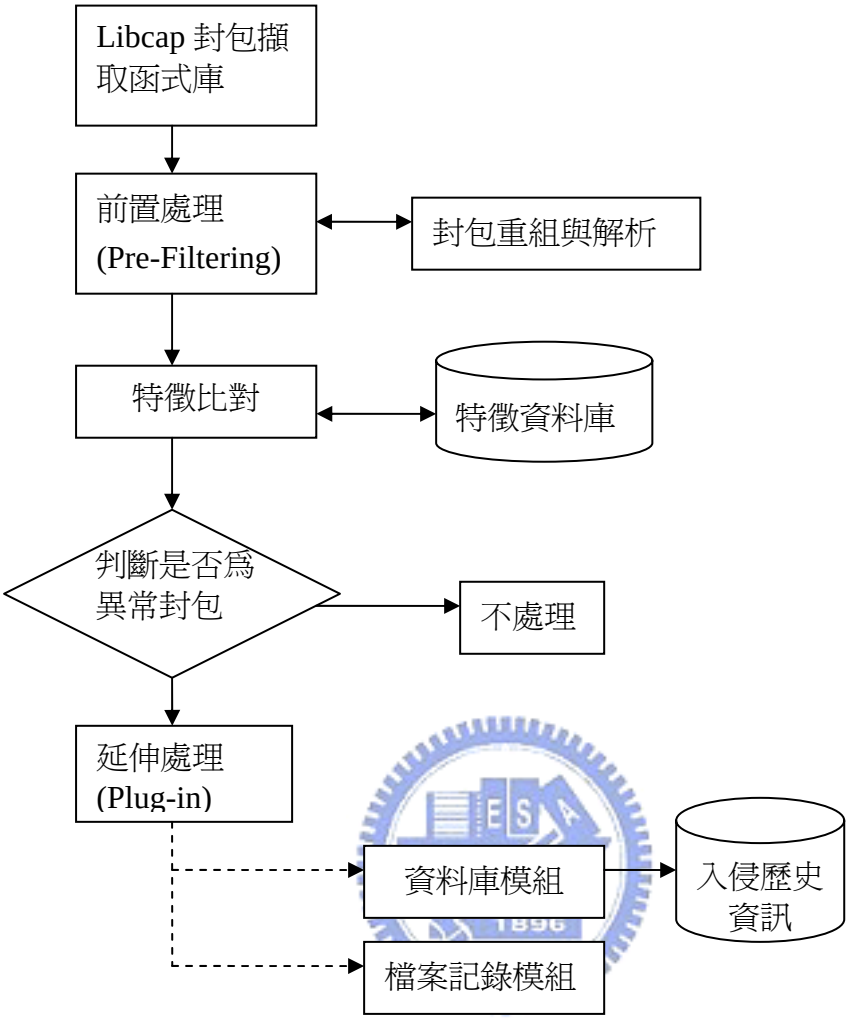

圖 4-1　Snort 運作流程圖

將系統流程簡化後，Snort 共可分為三部分: 1：前置處理(Pre-Filtering)； 2：特徵比對(Signature Compare)； 3：延伸處理(Plug-in)； 考量到我們在第三章所歸納的系統需求，入侵反應重點在於處理偵測警告後的防禦策略，因此我們將增加另一個溝通模組到「延伸處理」部分，負責將警告傳遞給無基礎行動網路上的其他偵測系統。相對地，每個系統也需要一個「協調模組」，可以接收由其他偵測節點內延伸處理模組所發出的訊息，並判斷是否需要執行防禦策略。

其次，執行阻擋防禦的功能應置於 Snort 的「前置處理部分」，當封包解析完成之後，直接判斷是否來自攻擊來源，如此便可省卻特徵比對的處理時間，進而節省系統資源，其修改後的系統架構示意圖如下:

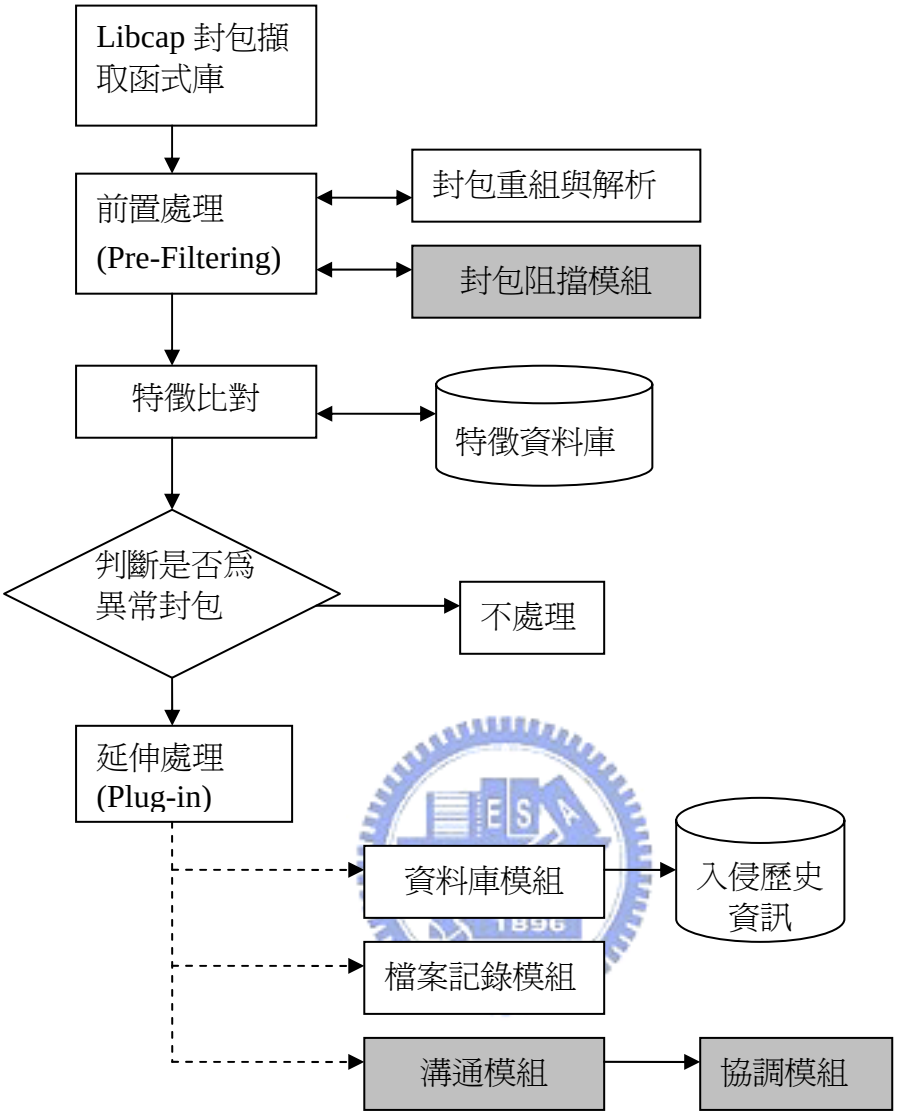

圖 4-2　Snort 修改後運作流程圖

灰色部分代表增加的功能模組，以期能達到入侵偵測與聯合防禦的估能，以下我們便針對新增模組功能進行深入探討。

4.2.1 封包阻擋模組

封包阻擋乃是執行整體防禦機制的第一線。當入侵偵測系統發現有入侵行為發生，判斷其入侵來源的 IP 位址後，便通知封包阻擋模組針對此來源 IP 傳送的

封包進行丟棄動作，如此便可節省特徵比對的時間與保護其他節點受到此種攻擊入侵的機會。特別是對於阻斷式攻擊而言，判斷 IP 來源所花的時間遠低於特徵比對的時間，當系統面對大量的封包湧入意圖癱瘓系統時，以耗用最低系統資源的方式將這些封包丟棄，便可達到維護系統安全之目的。

4.2.2 溝通模組設計

溝通模組目的在於通知其他入侵偵測系統，可疑的攻擊資訊，讓其他系統可預先警戒，提早進行防護策略，且避免重複偵測相同警告以節省系統資源。

模組設計上必須考量另一個問題: 避免濫發訊息反而造成整體網路的通訊品質下降，與阻塞網路流量。因此將訊息透過網路傳遞給其他系統前，有必要判斷警告的可信賴度，降低誤判與不必要送出的警告通知，避免入侵偵測機制本身對網路造成的不良影響。

最新經由 Snort 所公佈的異常特徵共有 1525 條，其中被列為攻擊類型的封包，意即會對系統造成傷害的異常特徵約有 500 條，約佔 1/3。其他異常類型包括「可疑的網路流量封包」,「掃瞄類型封包」,「偵測系統漏洞」,「使用異常網路阜」;「不符合字串標準」,「可疑存取行為」,「異常網路控制」等不會造成迫切問題，卻有可能為發動攻擊入侵前置準備的異常類型。

就系統安全的角度來看，即時捕捉有入侵危險的封包最為重要，實務上，當發現有實際攻擊行為時，可能某些系統已遭到入侵或因此受到影響，造成網路整體運作出現問題。因此針對可疑的網路異常行為過濾，進行阻擋防禦，有其必要性存在。

- 異常特徵分類

首先我們必須先針對偵測系統所發出的警告進行分類，將確實會對系統造成危害的入侵警告，透過網路通知其他偵測系統。而次一等可能造成潛在問題的封包則經過系統評估後才決定是否要傳送給其他入侵偵測系統。下表將異常特徵分群後，系統判斷是否進行溝通的對照表:

表 4-1　異常特徵分群

封包類型	系統判斷
攻擊類型封包	通知其他入侵偵測系統
偵測系統問題	系統判斷
掃瞄系統提供的服務	系統判斷
無特定類型	不處理

系統判斷的部分，由於無基礎行動網路有「能源消耗」與「運算速度較低」的系統需求，使用複雜的分析判斷方式反而會造成執行效率不彰，增加系統運算負擔的問題，且若要達到整體網路的入侵防護機制，必須在每個節點上均進行分析與評估運算，如此一來造成的系統負擔將更嚴重，拖慢整體無基礎行動網路的運作能力。因此，在本論文中採取較為簡單的方式，計算異常警告的次數，輔以門檻值檢定，當可疑的入侵來源觸發非直接攻擊異常類型超過門檻值時，系統便將此行為定義為入侵攻擊，採取防禦策略並通知其他入侵偵測系統進行聯合防禦。

- 門檻值檢定

實際觀察經由 Snort 在交通大學網路環境下所發出的警告訊息，可以發現一

個現象，分類為危險性最高的攻擊類型封包出現率相當低，約不到 1%，但這並不代表目前網路是安全的，因為目前屬於公司或學校的大型區域網路內，多半設置有防火牆與基本入侵防禦裝置，在安全裝置的過濾下，普通的攻擊類型封包無法進入，因此收集的警告多屬於掃描或搜尋網路弱點等低危險性的封包，其中觀察這些類型的封包又可發現當網路流量較高時，偵測到的異常類型封包也較多，如下圖所示:

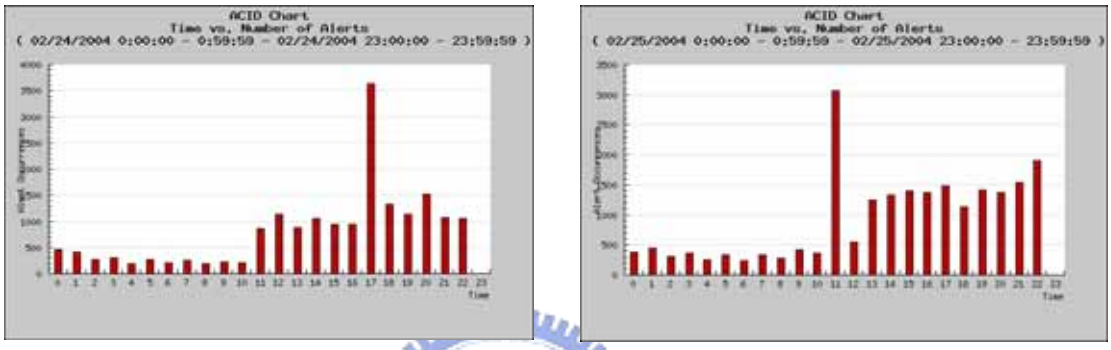

圖 4-3　Snort 偵測交通大學內網路異常狀況記錄

在某些非特定時段，會發生警告數量突然暴增情況。高密度的異常訊息可能代表有頻繁的攻擊行為，如病毒蠕蟲攻擊，或阻斷式攻擊等。再考量每天平均偵測的警告訊息約在 5000~20000 左右。若入侵偵測系統發出警告直接透過溝通模組對網路上的其他入侵偵測系統送出廣播訊息，容易會造成網路阻塞問題，且若發生阻斷式攻擊，這樣無異於幫助攻擊者達到癱瘓系統之目的。因此透過設定門檻值的方式，過濾低密度的異常封包，降低誤判機率，同時也減輕網路負擔。

由於每個不同時段所發生的警告數量並不固定，採用固定的門檻值難以反映網路目前狀況，因此我們參考第二章文獻探討中的「Adaptation techniques for intrusion detection and intrusion response systems」[15]中所提出概念，一個良好的入侵反應機制，應具備一定程度系統判斷能力，依照狀況而有不同的判斷依據。我們將文獻中所定義需系統介入判斷的部分列入考量，並依照現有系統的架構不同而進行修改，所產生的對應比照表如下:

表 4-2　系統加入適應型入侵反應考量的對照表

系統自動判斷的部分	實務設計上的對照
判斷警告是否可信賴	此部分由於溝通模組與偵測模組同樣包含於入侵偵測系統，安全性問題，因此不需考慮偵測模組所發出的異常警告是否有誤，是可信賴的。
依照警告類型進行防禦	使用異常警告分群的方式，攻擊性警告不需判斷，直接通知阻擋模組進行防禦策略，而可疑的警告則使用門檻值的檢查方式決定是否需要阻擋防禦。
採取何種防禦策略最為有效	最簡單有效的防禦策略，便是針對入侵來源進行阻擋過濾動作。同時考量到無基礎行動網路對於低成本的需求。因此論文中不使用較複雜的過濾方式。

透過動態門檻值設定，系統經由歷史的異常警告資料，決定目前門檻值，能符合不同的網路狀況，藉以判斷可疑的入侵來源是否符合攻擊條件。擷取歷史資料方面，若含入太舊的資料一併計算，不但浪費系統運算資源，也不符合動態調整門檻值的方法，因此我們只計算一段時間(Timestamp)內的警告資料作為計算門檻值的依據。門檻值計算公式採用資料分群法，找出分離點(Outlier)的公式:

$$\text{門檻值(Threshold)} = \text{平均值(u)} + [\ \lambda\ *\ \text{標準差}(\sigma)\ ]$$

平均值: 一段時間內，所有入侵來源所被偵測出的異常警告數量的平均值。

標準差: 一段時間內，所有入侵來源的異常警告數量間的標準差。

門檻值設定透過馬可夫不等式(Markov’s Inequality)的轉換，變成下列公式:

$$Pr[\ |\ X-u\ |\ >=\ \lambda\sigma\ ]\ <=\ 1/\lambda^2$$

若 λ 依照標準的分群公式，λ 設定為 3，代表在此段時間內，異常類型的封包中最高有 1/9 的機率超過門檻值而被判定為攻擊類型。透過門檻值檢定，我們從「可能為攻擊者」的來源 IP 中，經過濾後取出入侵次數較多的來源 IP，發送警告阻擋訊息。降低了因濫發訊息而造成整體網路的通訊品質下降，與阻塞網路流量的潛在問題。

因為檢定實際發生入侵行為與攻擊之前的異常狀態十分困難，需要長期的異常記錄與統計分析，且針對異常封包與實際入侵關係的最佳化並非本篇論文的重點，故不深入討論，在此架構下依照門檻值降低誤判機率的方式，作為發送警告訊息的依據。

4.2.3 協調模組

協調模組，主要用來處理由其他節點的入侵偵測系統所傳來的警告訊息，因為這些網路異常狀況經過警告分類與門檻值檢定篩選，可信度較高。入侵偵測系統在收到訊息後，對這些攻擊來源進行阻擋防禦可防止系統受到侵害。協調模組設計上需考量的問題為:

1. 節點之間不需先建立連線即可以傳遞資訊
2. 可能有偽造警告訊息傳入造成誤判，阻擋錯誤的資料來源

問題 1 的解決方式較單純，系統設計上透過 UDP 封包將警告訊息廣播給所有無基礎行動網路的節點即可，因為警告訊息的數量已過濾降低，對網路造成的負擔較小。

問題 2 的解決方式，在本文中以第三章所討論的多數決投票(Majority Vote)，作為協調模組的決策根據。

(發出警告的節點 / 網路的全部節點) > 0.5

每個的節點可以自由發出是否針對某個入侵來源進行阻擋的警告訊息，由協調模組負責計算與評估，考量到可能有偽造警告訊息，不能只接受任一節點的訊息即做出判斷，若發出警告的節點超過網路全部節點的半數才接受，並通知前端阻擋模組進行防禦策略。

4.3 系統架構

模擬一個可運作於無基礎行動網路的架構，我們依照前面章節討論與定義的系統需求與模組設計，系統示意圖如下:

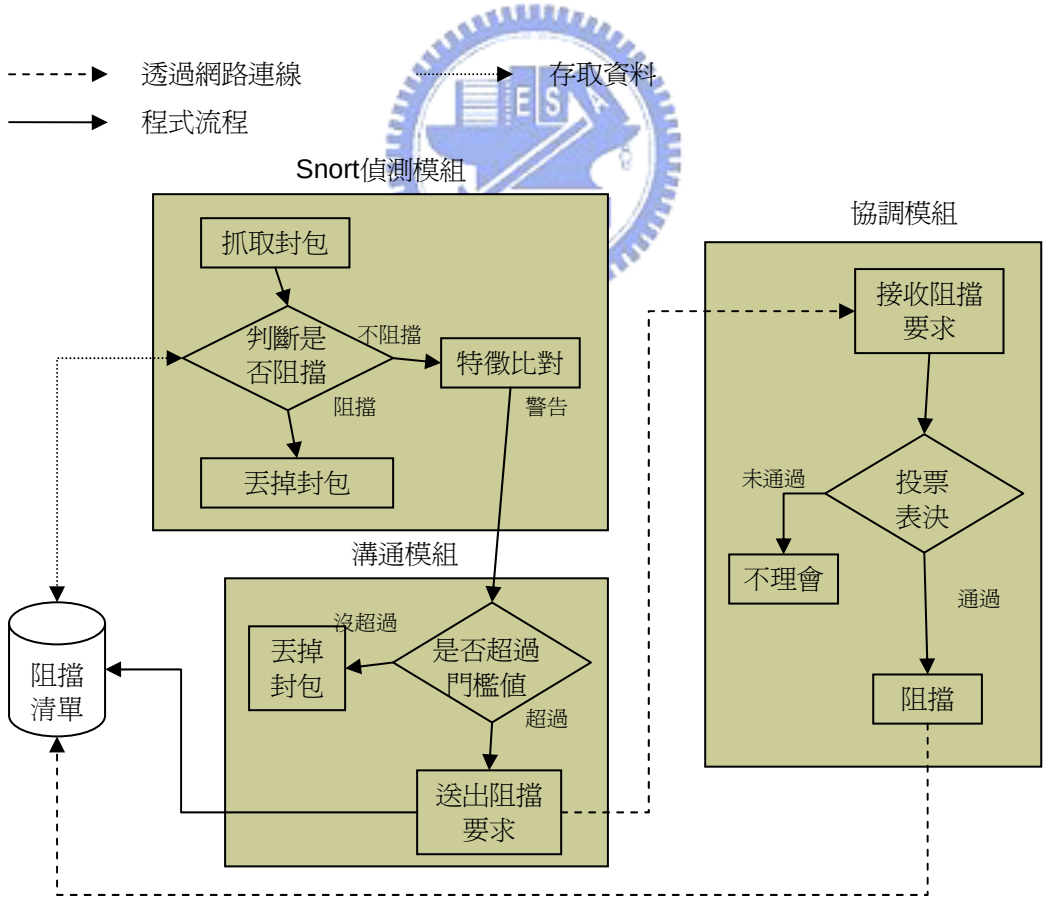

圖 4-4　聯合示偵測系統架構示意圖

系統架構共分為三個部分，其中偵測模組與溝通模組並存於「入侵偵測系統」內，協調模組乃是一隻獨立的程式，負責接收前端系統所發出的警告訊息。阻擋模組的實作透過『阻擋清單』和入侵偵測系統中的『前置處理』部分進行判斷，若符合阻擋清單所列的來源位址，則丟棄該封包。

溝通模組，負責接收前端偵測模組比對得到的網路異常訊息，經過『異常特徵分類』與『門檻值判斷』，若決定發出阻擋要求，則將攻擊來源 IP 存入阻擋清單，並使用廣播方式通知其他節點的協調模組。由其他節點的協調模組自行判斷是否對此來源進行阻擋防禦。節點間的訊息溝通示意圖如下所示：

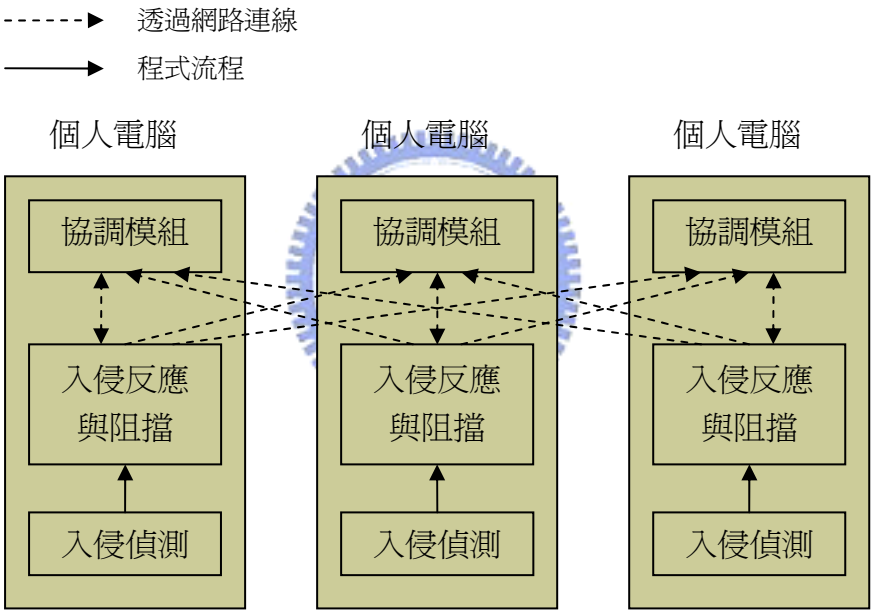

圖 4-5　多點偵測協調架構圖

4.4 資料結構

由於程式上分為兩個部份，入侵偵測系統，與後端協調模組，因此資料結構也分為兩個部份列出如下：

- 入侵偵測系統部分

表 4-3　入侵來源紀錄 (陣列)

欄位	說明
Attacker IP	記錄可能攻擊者的 IP
Counter	記錄共出現了幾次異常封包

表 4-4　記錄變數 (系統變數)

欄位	說明
FW_threshold	判斷警告是否超過過去記錄的依據，每段 TimeStamp 都需要重新計算新的門檻值
Timestamp_T	判斷是否到達一段 TimeStamp，此變數記錄本次 TimeStamp 起始的時間的時間。

- 後端協調模組部分:

表 4-5　投票記錄 (陣列)

欄位	說明
Attack_IP	記錄被提出警告訊息要求阻擋的入侵來源 IP
Voter_IP_List	記錄有哪些屬於無基礎行動網路的節點發出警告訊息

4.5 安全性分析

在模擬系統實驗中，入侵偵測主要仰賴兩種方式，判斷異常封包是否為攻擊類型，第一種，若封包被偵測系統歸類為攻擊封包，直接啟動阻擋防禦機制。第二種，依照此來源被偵測異常的次數來判斷。因此我們可以推論，攻擊型封包會受到直接阻擋，因此網路可免於各種已知且已被定義特徵的攻擊型態。其次，以數量為攻擊手段的攻擊類型則仰賴第二種方式的檢定進行防禦，如下圖所示，如典型的「阻斷服務型攻擊」，與「偽造路徑型攻擊」，可透過門檻值的檢定而發現

異常，啟動阻擋模組，將攻擊與系統的其他正常節點隔離。

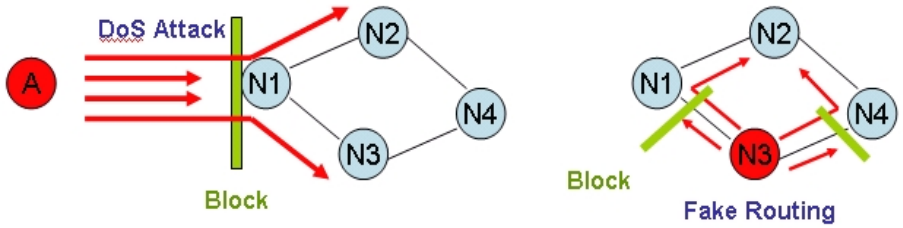

圖 4-6　系統對大量異常封包攻擊進行防禦的示意圖

4.6 效率分析

達到安全性目的並非針對無基礎行動網路的入侵偵測系統唯一需求，低成本，低資源耗損的要求對無線通訊網路也十分重要，因此我們透過執行時間的測試，評估增加了防禦機制後，入侵偵測系統所增加的運算時間。如下圖所示:

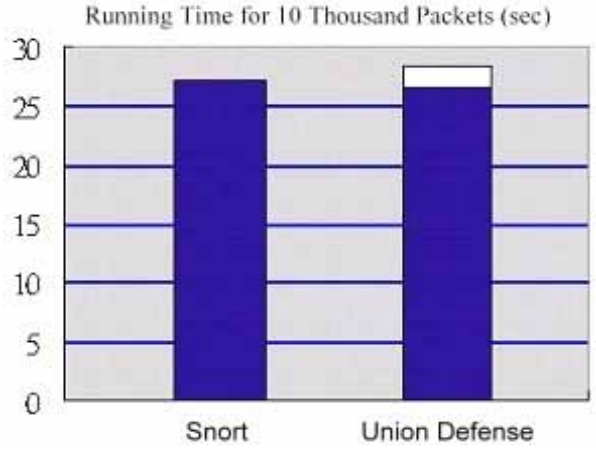

圖 4-7　偵測效率比較圖

在實驗中，分別對原始 Snort，與本次實驗修改的入侵偵測架構進行測試，估算兩個系統比對 10000 個封包所需的時間。

實驗結果: 在 AMD 1。3G，Window 2000 的系統下，Snort 每偵測一個封包平均需要 0.00275 秒，而實驗模擬的偵測系統平均需要 0.00283 秒，僅增加 3.5%的運算時間。但是當系統遭受攻擊時，只需花費 3.5%的時間就可決定是否將封

包丟棄不處理，在面對攻擊時便能發揮極大效果，同時成本增加的幅度不會造成系統過多負擔。

4.7 效能分析

效率評估後，另一個對入侵偵測系統而言十分重要的指標，便是系統偵測異常的準確率，亦即偵測系統在抓取封包，經過特徵比對發現異常的命中率。在一般情況下，網路流量不高時，入侵偵測並沒有因來不及處理而遺失封包的情況，但是在流量極大時，便有可能發生，而造成偵測系統的準確率降低。因此，我們參照一般應用系統測試系統所能承載服務人數上限的「壓力測試」方法，來檢查原始的 Snort 與修改後的入侵系統偵測的正確率是否符合預期表現：壓力測試的畫面如下圖所示：

圖 4-8　壓力測試畫面

在實驗中，我們讓偵測系統運作於一個流量極大的網路環境，平均每秒傳輸

7MB 資料，在大量的封包流動中，不定時地由另一台電腦對偵測系統丟出 600 個異常封包，測試其偵測準確率。實驗結果如下圖所示:

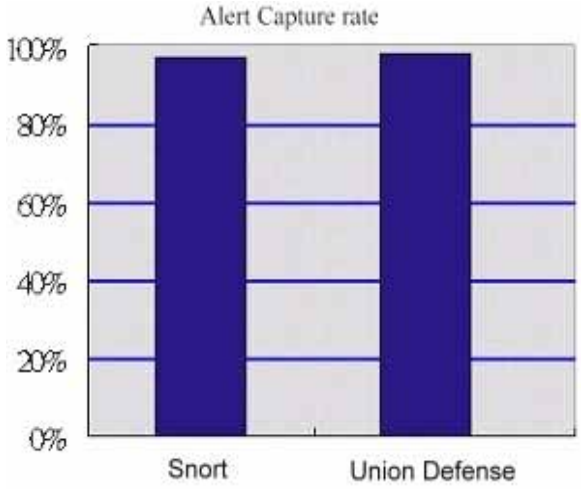

圖 4-9　偵測效能比較圖

原始 Snort 的偵測命中率約 97.2%，修改後的偵測系統命中率約 98%。兩者誤差極小，幾乎表現相同。由此可得到結論，加入了阻擋防禦機制的偵測系統，並不會影響其偵測異常的命中率。

4.8 小結

透過本章節的推論與數據，我們可以看到為入侵偵測系統加入防禦機制的成效與可行性，對於增加無基礎行動網路的安全性而言具有正面幫助。儘管增加了些許的系統運算時間，但面對入侵攻擊時，卻可有效地增加系統防禦能力，維持網路的安全性與穩定性。

結論說明瞭一件事: 建構一個聯合防禦式的入侵偵測系統，運作於無基礎行動網路的動態環境是具有可行性與執行效率的。

第五章　結論及未來發展

5.1 結論

本論文主要貢獻為建構一個應用於無基礎行動網路的聯合防禦式入侵偵測系統，包含自動反應機制，阻擋防禦策略，與節點間的溝通方式。實驗結果顯示系統可增加網路的安全性，預防、隔離有問題的入侵來源。無基礎行動網路本身具備移動性與便利性的優勢，節點間可自行構成網路並傳輸資料。這種自由的網路架構，不需花費固定裝置的時間與成本，即可達到通訊需求。但此種自由同時也犧牲了安全性，無線網路由於沒有實體線路，已存在許多資料安全與網路安全的問題，無基礎行動網路的動態架構，更使得防護資訊安全第一線的認證與加密機制運作困難，效率不佳，需要屬於第二線的入侵偵測系統輔助加強，才能維持良好的安全性。

在本論文所提出的系統實作，修改 Snort 成為一個可實用於無基礎行動網路的聯合防禦式入侵偵測系統，達到防堵阻斷式攻擊，偽造路由攻擊等異常攻擊狀態。在執行效率上僅增加原本入侵偵測系統的 3.5% 運算時間，執行效能維持與原系統相同，沒有增加系統的多餘負擔的疑慮。低運算成本的優勢在無線裝置上十分重要，而且 Snort 本身為開放架構的免費軟體，開發成本極為低廉，不需增加額外的硬體費用即可安裝，因此在實務應用上有較佳的成本優勢。

5.2 未來發展

未來可從無基礎行動網路的安全議題上著手的部分，包括從異常警告中發掘與攻擊特徵相關性的資料探勘方法； 加強節點間通訊的加密機制； 發展可運作於無基礎行動網路的認證機制，用來加強偵測系統間的溝通能力； 使用新制訂的 IDMEF 格式來溝通不同偵測系統間的訊息.

參考文獻

[1] D. Curry，H. Debar "Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML) Document Type Definition," draft-ietf-idwg-idmef-xml-06.txt，February 2002.

[2] E.H. Spafford and D. Zamboni, "Intrusion Detection Using Autonomous Agent," Computer Networks, vol. 34, issues 4, pages 547-570, 2000.

[3] J.R. Winkler, "A Unix Prototype for Intrusion and Anomaly Detection in Secure Networks," Proc. 13th National Computer Security Conference, Washington, D.C., Oct. 1990, 115-124

[4] Jiahai Yang, P. Ning, X, Sean Wang, and Sushil Jajodia, "CARDS: A Distributed System for Detecting Coordinated Attacks," In Proceedings of IFIP TC11 Sixteenth Annual Working Conference on Information Security, pages 171-180, August 2000.

[5] Krzysztof Zaraska "Prelude IDS: current state and development perspectives," http://www.prelude-ids.org/

[6] M. Conti and S. Giordano, "Mobile Ad-hoc Networking," In Proceedings of the 34th Hawail International Conference on System Sciences, 2001.

[7] Mishra, A.; Nadkarni, K.; Patcha, A. "Intrusion Detection In Wireless Ad Hoc Networks," IEEE Personal Communications, Volume: 11 , Issue: 1 , Feb. 2004 Pages:48 - 60.

[8] M. Scott Corson, Joseph P. Macker and Gregory H. Cirincione, "Internet-Based Mobile Ad Hoc Networking", *IEEE Internet Computing*, July‧August 1999, p.63-p.70.

[9] Mark Slagell, "The Design and Implementation of MAIDS (Mobile Agents for Intrusion Detection System)," M.S. thesis, Computer Science Department, Iowa State Universite, 2001.

[10]Martin Roesch. "Snort - Light weight Intrusion Detection for Networks," http://www.snort.org

[11]Matthew S. Gast "802.11 Wireless Networks: The Definitive Guide," 2003 Second Edition

[12]Nen-Fu Huang, "Design of Union Defense System for Localized Network Security", TANET 2002

[13]Parker, J.R "Voting methods for multiple autonomous agents" Intelligent Information Systems, 1995. ANZIIS-95. Proceedings of the Third Australian and New Zealand Conference on , 27 Nov. 1995

[14]Philip A. Porras, and Peter G Neumann, "EMERALD: Event monitoring enabling responses to anomalous live disturbances," In Proceedings of the 20th National Information Systems Security Conference, pages 353-365, Baltimore, Maryland, USA, National Institute of Standards and Technology/National Computer Security Center, October 1997.

[15]Ragsdale, D.J.; Carver, C.A., Jr.; Humphries, J.W.; Pooch, U.W. Systems, Man, and Cybernetics "Adaptation techniques for intrusion detection and intrusion response systems" 2000 IEEE International Conference on , Volume: 4 , 8-11 Oct. 2000 Pages: 2344 - 2349 vol.4

[16]S. Cheung, R. Crawford, and M. Dilger et al., "The Design of GrIDS: A Graph-Based Intrusion Detection System," Technical Report CSE-99-2, U.C. Davis Computer Science Department, January 1999.

[17]S.R.Snap. "A system for distributed intrusion detection[C]." Proc., IEEE Compcn 91 170-176.

[18]李勁頤，陳亦明，“分散式入侵偵測系統研究現況介紹”，資訊安全通訊 2002，Vol. 8