行政院國家科學委員會專題研究計畫　成果報告

一個針對無基礎行動網路的入侵偵測系統設計與模擬

計畫類別：個別型計畫
計畫編號：NSC93-2416-H-009-010-
執行期間：93 年 08 月 01 日至 94 年 07 月 31 日
執行單位：國立交通大學資訊管理研究所

計畫主持人：羅濟群

計畫參與人員：黃俊傑、楊仁豪

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 94 年 9 月 23 日

行政院國家科學委員會專題研究計畫成果報告

一個針對無基礎行動網路的入侵偵測系統設計與模擬

A Network-based Intrusion Detection System for Mobile Ad Hoc Networks

計畫編號：NSC 93－2416－H－009－010－
執行期限：93 年 8 月 1 日至 94 年 7 月 31 日

主持人：羅濟群　　國立交通大學資訊管理研究所
計畫參與人員：黃俊傑、楊仁豪　　國立交通大學資訊管理研究所

中文摘要

無基礎行動網路它是由一群具有無線設備的機器平台，在任一個地方或時間，可依其需要而建立起一個互連的網路架構，因此，它具有高度的機動性與自我組織能力。因為有上述的特性，使得它非常適用於急難救助與軍事戰場上。

在此網路平台上雖具有上述的優點，但由於具有動態拓樸，使得舉凡路由問題、服務品質保證問題與資訊安全問題等等，都與無線網路所討論的架構有所不同。本研究將針對資訊安全之入侵偵測問題，設計一個符合無基礎行動網路環境所需的架構。在入侵偵測的相關研究，除了核心的入侵偵測方式，應用在點對點網路，需要考慮節點間資訊交換的完整性，與共同分擔偵測的機制，在整體性的考量下，其研究才具備可行性。

基於上述的概念，本研究提出一個可行的架構，稱之為聯合防禦式的入侵偵測機制，於此機制下，所有成員除了處理本身的入侵偵測外，亦將可能的攻擊資訊送至其他成員，每個成員採多數決的門檻分析模式，藉以判斷可疑的入侵是否為攻擊來源。另於系統實作部份，修改 snort 作為讀取封包的來源，並以分散式的入侵偵測機制為基礎，結合入侵反應機制，使其達到聯合防禦之目的。最後，藉由安全性分析與效率分析，說明本研究所提的架構之安全性與可行性。

關鍵字：無基礎行動網路、入侵偵測、入侵反應、聯合防禦

Abstract

Mobile ad-hoc networks, MANETs, are a network topology which combines the wireless devices into an infrastructure-less environment. And all nodes, i.e. wireless devices, have high mobility and self-organized ability. To have such properties, the MANET is more suitable in emergency and battle field.

Though the MANET has the above advantages, its dynamic topology makes the problems such as routing, quality of service and information security more different than the current wireless network. In our research, we focus on information security problem and design the intrusion detection system that satisfies the MANET environment. In the study of intrusion detection scheme in MANT, the intrusion detection methods is the one of the topics we must concern, but the related researches like the integrity of data exchange and cooperative detection mechanisms are required to make the system more feasible.

In our research, we propose a union-defense-based intrusion detection mechanism which is supported by majority vote to make a decision whether performs union defense or not for MANET. The system implementation is based on distributed intrusion detection system with intrusion response, message exchange, and union defense scheme to enhance network security and system stability and protect the MANET from malicious attack and denial of Service (DoS) attack. The security analyses and performance analyses present the scheme we proposed is securer and more efficient than the others.

Keywords: Mobile Ad-Hoc Networks, Intrusion Detection, Intrusion Response, Union Defense

一、緣由與目的

本計劃是延續前一年「無基礎行動網路環境下身份認證與安全群播機制之研究」研究成果。在該計劃中我們完成了在無基礎行動網路架構下，以具有雙向身份認證為基礎下的安全群播環境探討。

然而，在此環境中由於節點間的通訊並不須預存一個基礎網路的設置，它們彼此間能自我組成(Self-Organize)完成構連，建立起通訊管道，而當兩個節點間已超過無線電電波範圍(radio range)，則另一個節點立即具有路由功能，藉此搭起兩通訊機之間的通訊通道。因此，它是一個具有多階性、動態拓樸與不可信賴的通訊通道。故在此架構下，資訊安全問題顯得特別複雜且重要。例如，若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，例如:藉由傳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。因此，本計劃針對安全性問題進一步探討，在無基礎行動網路環境中遭受入侵時的應對機制，進而提高系統存活度，相關議題包括建立偵測入侵機制、訊息交換與聯合防禦的方法。

將網路安全從攻擊時間的角度來分析，切割成事前、事發、事後與事終。其中事前，進行資訊驗證；事發，進行入侵偵測；事後，資訊存活及事終，資料鑑識。過去幾十年來，已經有非常多的學者投入事前身份驗證機制的設計，但由於目前攻擊種類更為複雜，因此，無法單靠預防就能處理。所以，第二線的防禦工作－入侵偵測機制的設計，就顯得相當重要。

現有的入侵偵測系統，依架構大致可區分成網路型(Network Based IDS, NIDS)、主機型(Host Based IDS, HIDS)及分散型入侵偵測系統(Distributed Based IDS, DIDS)；除此之外，在功能上亦增加了很多，例如加入了動態分析、誘捕、自動反應等等，大幅的增加了入侵偵測系統的效能。但由於各種不同屬性或功能的入侵偵測系統，都有其適用環境，及其優缺點存在。例如，適用於有線網路環境的入侵偵測系統將其移植到無線網路環境，會因為無線網路的特性，包括網路傳輸的延遲性、運算速度慢等問題，而導致偵測效果不佳的現象發生。

無基礎行動網路，它除了具有無線網路的特性外，又由於它具有動態拓樸的特性，使得節點的加入與離開都較為複雜；且因為它具有多階性，使得若某一節點遭受攻擊，將產生遞移效應，故於第二道防線的入侵偵測機制設計上，又與其他的無線網路不同。因此，本研究將針對無基礎行動網路的環境，設計一個符合此環境需求的防禦機制與遭受入侵時的應對方法，以提高網路安全與系統穩定度。

二、文獻探討

本小節將就無基礎行動網路環境、在此環境常見的入侵攻擊及入侵偵測機制與現有的相關系統做概略性文獻討論。

2.1 無基礎行動網路環境

在無基礎行動網路環境中，節點間可以做直接的通訊，也能隨意移動，並繼續保持節點間連線的狀態。無基礎行動網路是由無線裝置自行建立的區域網路環境，其中並無無線擷取器或橋接器，它是一種能夠在沒有事先建置基礎架構的環境下，讓各個節點透過彼此點對點連結所臨時組成的網路，使得節點間彼此之間能夠互相傳送資料。

而無基礎行動網路最主要的特色包括動態拓樸及具有自我組織的能力[5] [7] 。

由於動態拓樸的特性使得各個連結設備可以任意移動位置，且還能和其他節點繼續溝通；具有自我組織的特性，使得一方面它不但可以簡化網路的管理，提高其強健性(robustness) 和彈性，另一方面，它更能在動態的狀況下，像位置移動、不定的連結、和無法預測的流量負載的既定基礎結構下，作最理想的資源有效使用。

2.2 無基礎行動網路常見的入侵攻擊

在無基礎行動網路環境中，雖有第一道的身份認證機制，但有些攻擊的目標並不是在取得身份認可，侵入系統，而是藉由傳送大量的封包或其他方式而達到入侵攻擊之目的。因此，本小節即就此類攻擊做討論。

於[4] 文中, 即就應用在無基礎行動網路環境中可能遭受的攻擊，做詳細分類，包括：黑洞問題(Black Hole)、阻斷式服務攻擊(Denial of Service, DoS)、路由溢位攻擊(Routing Table Overflow)、偽冒節點問題(Impersonation) 與消耗電力(Energy Consumption)等問題，如下圖 一。

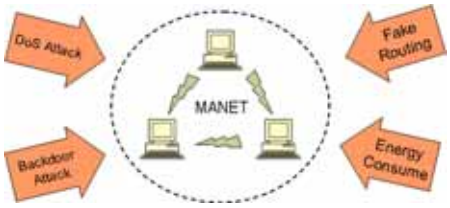

圖 一：無基礎行動網路常見的攻擊

- 黑洞問題：由於在無基礎環境中，任何一個節點既可當一般主機亦可當路由主機的角色；當某一節點欲與另一節點要建立一個路由路徑時，若是採用 AODV(Ad hoc On Demand Distance Vector)的路由機制，則每次有路由路徑需建立時需詢問一次，因此，發送端需發送一個 RREQ 的封包給其鄰近的所有節點，然後依此詢問下去，直至目的節點或是某一中間節點可以協助完成後續的路由建置為止；然後，再由目的節點或是該中間節點傳送一個 RREP 的封包至原始發送端便完成路由的建置。上述為正常的路由建置程序，但若有一個惡意的節點，宣稱自己具有最短的路由資訊，使原始節點對於最短路徑的判斷產生錯誤，而誤信此惡意的節點，例如，下圖 二中假若節點 1 欲與節點 4 建立一個路由路徑，而節點 3 是一個惡意的節點，假若節點 3 回送一個 RREP 的訊息，由於節點 1 會認為它是最短路徑，而將資料傳送給他，這就是黑洞問題。

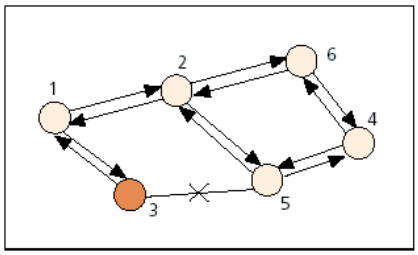

圖 二：惡意節點的黑洞攻擊[1]

- 阻斷式服務攻擊：該攻擊即藉著發送大量的封包，使得網路頻寬被佔滿或是導致提供服務的主機無法正常提供服務。
- 路由溢位攻擊：即攻擊者提供一份假冒路由資訊表給原始節點，使其原始節點誤信該路由表，而將資料傳送至不存在的節點，因此，所有的資料就無法順利的背送至目的地，其攻擊方式如下圖 三。

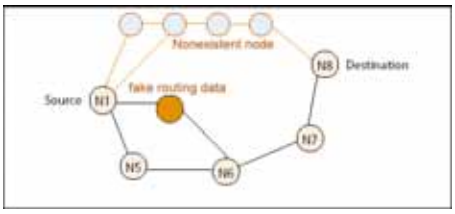

圖 三：路由溢位攻擊模式

- 偽冒節點：惡意的攻擊者偽冒一個合法的節點，並傳送一個控制封包來修改現有的路由資訊表，最後，將導致所有的資訊都會經由它傳遞至目的節點，因此它可以擷取所有的傳送資料。例如，下圖 四即惡意的攻擊者偽冒合法的節點 4, 並送出一個控制封包來修改路由資訊，使得所有由節點 1

送出至節點 8 的資料都會被竊取。

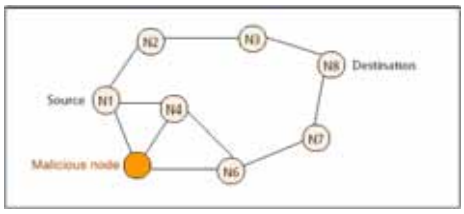

圖 四：偽冒節點攻擊

- 消耗電力問題：對無線網路而言，電力問題一直都是他們非常重視的項目，因此，盡量只傳送必要的資訊；假若某一個攻擊者，一直要求鄰近的節點協助傳送無必要的資訊，將導致電力耗損相當可觀。

2.3 入侵偵測系統

在無基礎行動網路環境中，由於具有動態拓樸、運算效率較低與多階性的特徵，使得該環境更容易遭受攻擊者以傳送大量封包作為攻擊的方式，因此，需要有一套符合該環境需求的入侵偵測機制。

在入侵偵測設計上，必須考量的項目包括資料來源的收集、依收集到的資料作入侵分析以及最後將其分析結果回報至管理者或網管系統上。在資料來源的收集上依架構可分成主機型及網路型的資料收集方式。

- 主機型資料收集：藉由監視系統的運作紀錄，例如 Win2000 環境中安全日誌記錄，找出可疑的攻擊行為，若有事件發生時，主機型的入侵偵測系統即作入侵行為的比對，若有符合，則由回應模組通知系統管理者，以做出適當的反應。
- 網路型資料收集：以原始網路封包作為資料來源，然後攔截所有過往的網路封包，以進行偵測及分析，作為判斷是否遭受攻擊者攻擊或是入侵的依據。網路型入侵偵測系統有一優點即是不管在此網路環境中有多少種的作業系統，由於在相同的通訊協定下，封包格式一致；所以，可以很簡單的藉由檢查封包的標頭，來判斷是否為一個攻擊封包。因此，網路型入侵偵測系統具有較佳的彈性，其缺點就是由於要處理大量封包，故 CPU 處理效率就顯得特別重要；另外，若網路上的封包已經加密過，則網路型的入侵偵測系統無法適用。

若依入侵分析模式來區分，可分成誤用檢測型(Misuse Model)與異常檢測型(Anomaly Model)兩大類。

- 誤用檢測型模式：它是利用已經收集到的資訊來建立各種攻擊模式，再依此作為比對判斷其行為是否為攻擊行為，亦即是說，它建立了正面行為模式(Positive Behavior Model)，此種方式的誤判率較低，但缺點即是若現行的攻擊行為不存在攻擊模式的資料庫中，將無法偵測此行為。
- 異常檢測型模式：它是屬於一種負面行為模式(Negative Behavior Model)，亦即系統建立正常行為模式資料庫，將所偵測到的行為與現存模式進行比較，若差異太大，則視為異常行為。

在回應模組部份，可分成被動式與主動式兩種；其中，被動式機制，即是產生警告訊息通知網管人員，但此種方式由於系統本身不具有評估與判斷力。然而，隨著攻擊模式的複雜化，攻擊程式也轉為半自動或自動的攻擊方式，此種攻擊方式以經令傳統的入侵偵測系統無法負荷，此時即需採取主動式的回應機制，或稱為入侵反應系統(Intrusion Response System, IRS)。當它發現網路貨主機遭受攻擊時，會採取必要的應變措施，因此，此系統的存在顯得特別重要。入侵反應系統可以分成三大類：提醒、手動反應與自動反應[2]；其中自動反應，可以做到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，達到安全防護的效果。

由上可知，入侵偵測系統是在偵測網路上異常的行為，而入侵反應系統，則在處理發現問題後的後續處理，做出反制動作。因此，必須兩者同時存在才是一個完整的系統防護機制。

另外還有一種稱為分散式入侵偵測系

統，最早出現於 1990 年，由 UC Davis 提出[9] ，其主要目的為追蹤使用者在網路內的移動，利用一個獨特的識別碼(NID)來追蹤使用者的行為。而它的架構是由單一電腦改變成多台電腦分析，因此，可以跨不同的網域，得到更多的資料以提供分析使用。其架構上它結合了主機型與網路型系統的特點，能至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。現有的分散式入侵偵測系統，例如，DIDS[9]、GrIDS[8]、AAFID[3]等等。此外，為了因應分散式架構的特性，由 IDWG 提交 IESG 審核的入侵偵測訊息交換格式(IDMEF)[1] ，它的目標是在制訂一個入侵偵測系統間訊息傳遞的公開資料格式標準，以滿足異質入侵偵測環境的要求。如此一來，當入侵偵測系統發現可能攻擊行為時，它可以將警告訊息以 IDMEF 交換格式（以 XML 格式描述定義）傳遞給其他入侵偵測系統或上層的管理系統。

三、研究方法

本研究是基植於無基礎行動網路環境下，因其特殊架構的需求所提的聯合防禦機制之入侵偵測與防禦系統，以達系統安全之目的。並藉由系統模擬說明其成效。以下即就本研究之機制與安全性分析做描述。

3.1 應用於無基礎行動網路之入侵偵測設計要求

本研究乃基於叢集架構下討論無基礎行動網路的入侵偵測系統。因無基礎行動網路具有的特性，使得入侵偵測系統在設計時會遭受一些困擾。

- 無階層式或集中式管理架構：由於傳統的分散式入侵偵測系統，是採一台伺服器負責收集與分析各個網域 agents 所送過來的資料，因此，無法將其直接應用於無基礎行動網路環境。
- 動態拓樸：如何確保入侵偵測系統可以不受節點移入與移出，而影響其執行校能，也是設計上考量的重點。
- 多階性：由於任一節點除了具有一般節點的角色外，還可以具有路由的功能，因此，如何防止節點成為入侵的跳板，也是設計上考量的重點。
- 電力問題：面對消耗性與癱瘓性的攻擊時，如何提供有效的應對機制是非常重要。

由上述可知，於架構上本系統需朝向分散式系統設計，將偵測器佈建於網路中各節點，才能達到完整監控之效果。另外，於入侵反應之機制上，由於在無基礎行動網路的環境並沒有如防火牆裝置可以過濾網路封包，且資料量與節點數量成正比，亦即是說，所有節點平均分擔整體網路流量。因此，假若可以將過濾與阻擋的功能整合於入侵系統本身，將防禦機制建構在每一個節點上，由入侵反應元件啟動防禦策略，以達到防護的效果，其架構如下圖五。如此一來，異常封包在經過有偵測系統的節點時會遭受阻擋，而不會再將此攻擊封包遞送至下一個節點，即可達到維護整個網路安全的目的。除此之外，於系統設計上需考量節點間可以互通，不需透過另一層的管理協調機制，即可傳遞資訊。

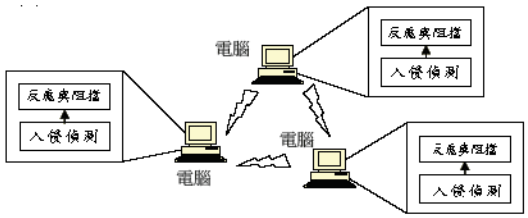

圖 五：結合入侵與反應的入侵偵測系統

3.2 聯合防禦機制

於上小節我們了解應用於無基礎行動網路之入侵偵測系統設計之要求，並已充分了解無基礎行動網路之特性後，我們以分散式架構為基礎，每個節點兼具有入侵偵測與入侵反應的機制，如此一來，就可以符合該網路架構的要求，本系統可以隨著節點的移動而進行入侵偵測，若節點偵測到有異常攻擊，本身可立即實施入侵防禦，又能將此異常資料傳送至鄰近節點，

共同執行聯合防禦機制。如此一來，其他尚未遭受此型態攻擊的節點，預先將此封包阻絕於外，而不用再執行一次入侵偵測，因此，可以節省該入侵偵測的時間。

由於本機制採用聯合防禦的特性，因此，節點間必須相互傳遞資訊，所以需考慮資訊交換的問題，以免因資料交換過頻繁，而導致網路擁塞問題。為了解決此問題，加入警告分類機制，過濾較輕微的入侵警告，將嚴重或危及的警告傳遞給其他節點，以降低因聯合入侵防禦機制所造成的網路負擔問題，其架構如下圖 六。

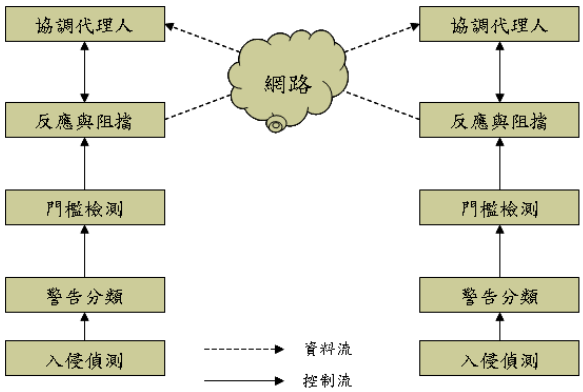

圖 六：聯合入侵防禦機制架構圖

以下就每個區塊功能做說明：

- 入侵偵測：本系統屬於網路形入侵偵測，本模組主要抓取網路封包，並比對解析是否為異常封包。
- 警告分類與門檻檢測：由於本系統於入侵偵測，採 snort[10] 作封包收集，但 snort 定義的規則過於詳細。因此，我們先就該規則做分類，分成異常攻擊警告、普通警告與輕微警告三大類；其中若屬於第一種分類，則該節點立即進行防禦策略，並通知網路上其他節點，以免遭受同樣的攻擊；若屬於第二種分類，主要針對網路掃描或弱點掃描，因為此種型態看起來不像第一種具有威脅性的攻擊，但有能在發現弱點後會進行更大規模的攻擊，因此，藉由門檻值檢測法進行篩檢，以減少因聯合防禦機制所產生網路封包的流量。
- 反應與阻擋：當某一節點執行入侵偵測，發現屬於攻擊型封包，立即執行防禦工作，將此封包丟掉，使其無法傳遞至網路上其他節點。
- 協調代理人：負責接收由其他節點所傳送的警告訊息。為了防止惡意的攻擊者製造假訊息，而讓入侵偵測系統執行不正確的防禦工作，所以，我們採用多數決的方式[6] 。亦即是說，不能只從單一來源的節點資料作為判斷依據，只有當發出同樣警告的節點數超過現有環境所有節點個數的半數，才接受此訊息。因此，單一攻擊來源無法偽造訊息而讓某一節點誤判。另外，此機制非常適用於動態環境的無基礎行動，因為多數決可以隨著成員的多寡作動態調整。其公式如下：

$$\begin{cases} \text{if } (\#\,Alert\ nodes)/(\#\,Total\ nodes) > 0.5\,; accept \\ \qquad otherwise; reject \end{cases}$$

3.3 系統設計與模擬

本模擬系統之設計是依據上述的聯合防禦機制的架構設計而成。於系統實作部分採 snort 作基礎，並新增三個模組，包括封包阻擋模組、溝通模組及協調模組，其架構如下圖 七：

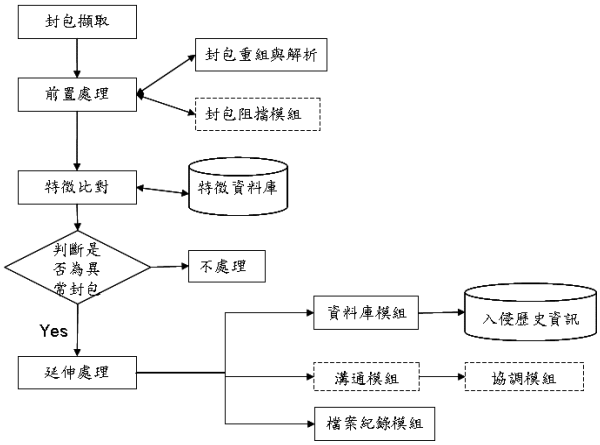

圖 七：入侵防禦系統架構

關於 snort 本身的模組由於篇幅的關係，在此不作詳述。以下即就本研究為達成在無基礎行動網路環境的聯合入侵防禦機制所新增的三個模組作細部說明：

- 封包阻擋模組：本模組為執行整體防

禦的第一線。當入侵偵測系統發現有入侵行為發生時，判斷入侵來源的封包標頭之 IP 位址後，立即通知封包阻擋模組針對此來源的 IP 位址進行阻擋，並丟棄此封包，如此可以節省至特徵資料庫進行特徵比對的時間，並且保護其他節點遭受此攻擊的機會。例如，在 DoS 的攻擊模式，採用此方式就可以達成維護系統安全的目的。

- 溝通模組：在聯合入侵防禦系統中，溝通模組扮演著非常重要的角色。它必須協助該節點通知其他節點的入侵偵測系統相關可能的入侵資訊，讓其他系統可以預先作防範。於系統設計上，為了避免發生該模組濫發訊息，造成整個網路壅塞，這對無基礎網路而言是嚴重的事件。因此，在訊息傳送給他人之前，必須自行判斷該警告的可靠度，以降低誤判且避免傳送不必要的警告訊息，以避免聯合入侵偵測機制所可能造成的網路運行效率問題。因此，在系統設計上需考慮系統安全與實務面兩者必須同時兼顧，故針對可疑的網路異常行為過濾，進行阻擋防禦，並送出警告訊息的系統環境設計有其必要性。為了解決上述問題，本研究於本模組設計上，加入異常特徵分類與門檻值檢定兩個機制。其中異常特徵分類即是針對入侵偵測系統所發出的警告進行分類。分類法則，即是將所有的警告分成三大類，分類法則請參照上述 3.2 小節之警告分類。因此，只要屬於第一類者，本身除執行防禦外，立即透過本模組通知其他節點。若屬於第二類者，則需藉由系統評估後才決定是否要傳送給其他入侵偵測系統。而於系統判斷上，為了避免因複雜的判斷法則，而導致消耗大量的電源，故本研究採計算異常警告的次數並輔以門檻值檢定法則，以過濾低密度的異常封包，降低誤判機率，並減低網路負擔。因此，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，系統即認定為入侵攻擊，採取防禦策略並通知其他入侵偵測系統進行聯合防禦。而於門檻值機制上，本研究採動態的門檻機制，故可依照狀況而有不同的判斷依據。所謂動態門檻值設定，即系統經由歷史的異常警告資訊，決定目前的門檻值。於公式計算上採資料分群法，以找出分離點：

$$Threshold(T) = \mu + (\varepsilon * \sigma)$$

有關 ε 參數的決定則透過柴比雪夫不等式(Chebyshev's inequality)來決定。例如，當 ε 設成 3 時，代表在此段時間內，異常類型的封包中有 1/9 的機率超過門檻值而被判定為攻擊類型。因此，透過門檻值檢定，我們從可能攻擊者的來源 IP 中，經過濾後取出入侵次數較多的來源 IP，發出警告阻擋訊息。故可以降低因濫發訊息而造成網路品質的降低。

- 協調模組：本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，且由於這些警告訊息是由原傳送節點經門檻值篩選，故可信度較高。於協調模組設計上需考慮兩個問題，包括：節點之間不需先建立連線即可完成資訊交換以及對於有可能偽造警告訊息傳入造成誤判的困擾之處理。關於第一個問題的解決方式，於系統設計上採 UDP 的封包格式，以降低網路負擔；第二個問題則採多數決的方式，作為協調模組的決策根據。亦即是說，每個節點都可以發出因入侵而產生的警告訊息，但各自節點是否接受此訊息，進而進行阻擋，此項行動是由協調模組負責計算與評估，而評估原則採多數決方式，即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。

3.4 系統架構

本小節將上述各模組的功能以下圖八來描述：

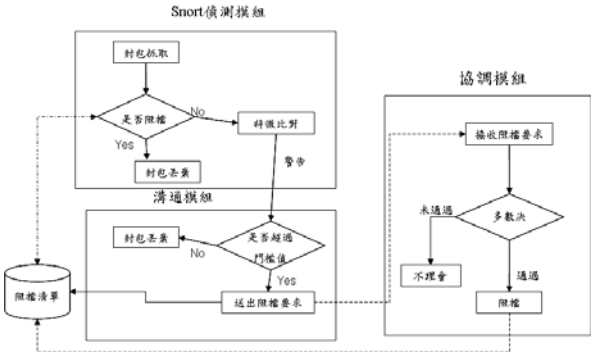

圖 八：聯合入侵偵測防禦系統架構圖

由上圖 八可知，本系統可分成三大區塊，其中偵測模組與溝通模組他們是並存於入侵偵測系統內，而協調模組是單獨的一個程式碼。其中協調模組負責接收前端系統所發出的警告訊息；阻擋模組於實作上是透過阻擋清單以及入侵偵測系統的前置處理，作為判斷封包是否該丟棄的依據；而溝通模組再接收到前端經由特徵資料庫比對為異常封包後，立即進行異常分類與門檻值判斷，以決定是否要發出阻擋要求，若是則除了進行阻擋防禦外，還需將此記錄寫至阻擋清單，並由廣播方式通知其他節點的協調模組，再由各自節點的協調模組內建的多數決程序，決定是否要進行聯合防禦。以下即是節點間訊息溝通的示意圖，如圖 九：

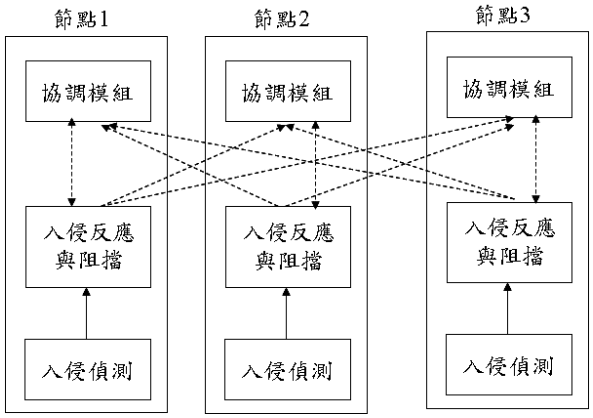

圖 九：多點偵測協調架構圖

下圖為本研究以三台電腦做為無基礎行動網路環境下的聯合防禦主機，我們發現藉由圖 十、圖 十一及圖 十二，可以證明投票機制是有發生作用，以阻擋來源攻擊，並於下小節，說明本研究於安全性與效能分析均滿足需求。

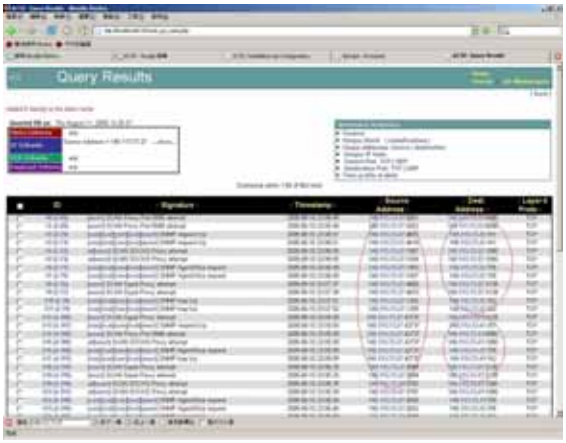

圖 十：攻擊資料的紀錄

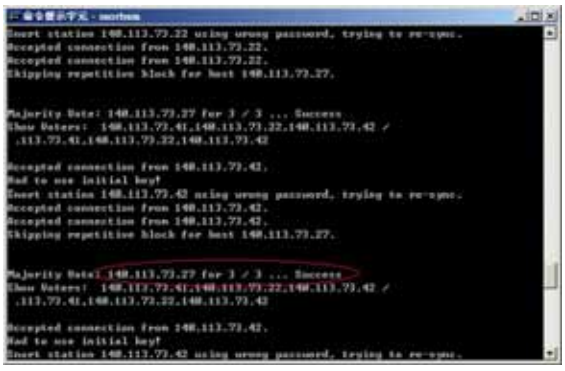

圖 十一：啟動投票機制

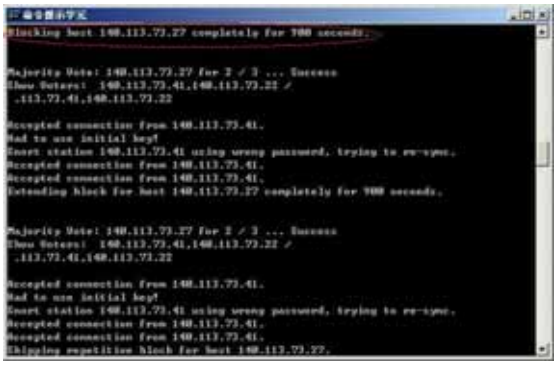

圖 十二：啟動聯合防禦機制

3.5 安全性分析與效益評估

本小節就本研究所提的聯合入侵防禦機制之安全性作分析，另就本研究的系統做效益評估。

於安全性分析方面，由於本研究所採用的機制於可疑封包分類上，共分成三大類。若被歸為第一類者，由於是屬於攻擊性封包，因此，立即直接進行封包阻擋，故可以完全免於各種已知且被定義特徵的

攻擊；若屬於第二類者，主要針對傳送大量封包的攻擊，例如 DoS（如圖 十三）與偽造路由路徑型態攻擊，都可透過門檻值檢定方式發現異常，並啟動阻擋模組，將攻擊封包阻絕於外，以防止影響到其他正常的節點。因此，本研究所提的聯合入侵防禦機制，可以滿足安全性的需求。

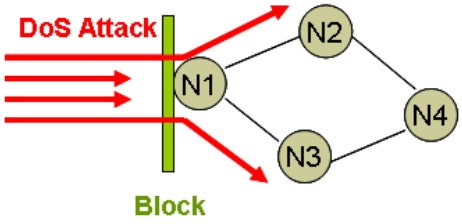

圖 十三：DoS 攻擊之阻擋防禦

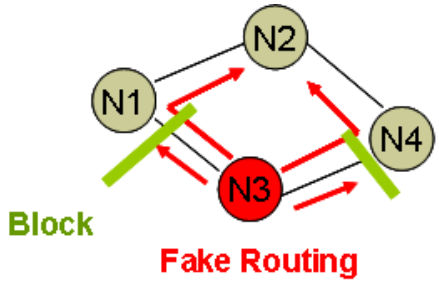

圖 十四：偽造路由路徑型態攻擊之阻擋防禦

除上述安全性問題外，效率與效能分析對無基礎行動網路而言是非常重要的。因為若我們可以提高入侵偵測系統的執行效率，就可以減低對電池的耗損。因此，我們透過執行時間的測試，評估本研究在增加了入侵反應的防禦機制後，其入侵偵測系統所增加的系統運行時間。其做法如下：我們分別在基本 snort 與聯合防禦的環境下各送出 10000 個封包，估算兩個系統比對 10000 個封包所須的時間。結果顯示，在基本 snort 的版本中，偵測一個封包平均只需要 0.00263 秒，而在聯合防禦的版本中，偵測一個封包需要 0.00269 秒，僅多花了 2.3%的時間在聯合防禦的動作上，因此，証明本系統之可行性。其結果如下圖 十五：

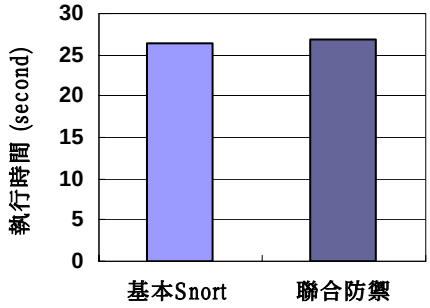

圖 十五：無聯合防禦與聯合防禦偵測效率比較圖

另於效能分析上，即是探討本研究所提的聯合入侵防禦機制於發現異常攻擊的命中率。尤其若網路環境處於流量極大的情況下，如何能確保本系統的準確率是非常重要的課題。因此，我們比較基本 snort 與聯合防禦版本的 snort 在抵擋攻擊上的動作上是否有相同的正確性，分別在相同環境的前提之下對兩各不同版本的 IDS 各丟五百個攻擊封包，冀望藉由發出警告訊息的數目，來得之實際的偵測率，以檢查原始 snort 與修改後的入侵偵測系統的正確率是否符合預期表現，其畫面如下圖 十六：

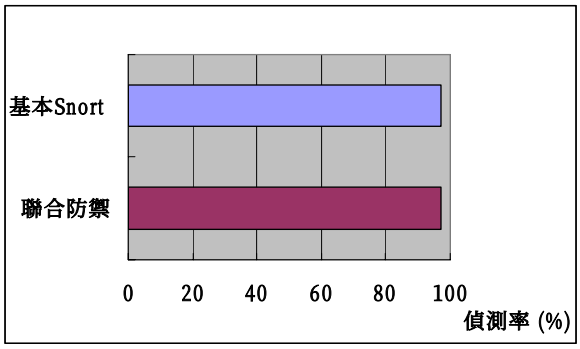

圖 十六：無聯合防禦與聯合防禦偵測率比較圖

結果在基本 snort 版本有高達 97.2%的偵測率，聯合防禦的版本也有 97%的偵測率，兩者可謂不分軒輊，也顯示了聯合防禦的版本是可行的。因此，由上的實驗結果可驗證本研究所提的聯合防禦入侵偵測機制，不論從安全性或是執行效率與效能的角度來看，都可以滿足無基礎行動網路

環境的要求。

四、結論與建議

無基礎行動網路因具有動態拓樸及自我組織之特性，使得它有別於其他無線網路架構，故可應用的範圍更廣。而入侵偵測機制，是整體安全的第二道防線。本研究所提的聯合防禦入侵偵測機制，它具有自動反應機制、阻擋防禦策略及可透過協調模組完成聯合防禦之效果，因此，非常適用於無基礎行動網路環境的要求。

另由實驗可證實，本研究雖新增了聯合防禦與節點自動反應阻擋機制，但於效率分析上可以發現其增加的負荷並不多，但卻增加了安全面與提升了異常偵測的命中率。尤其本研究於實作上是修改 snort 再新增三個模組而成，由於 snort 本身為開放架構的免費軟體，開發成本低廉，因此，非常適用於實際環境的要求。

另本研究未來可以就節點間訊息傳遞的部分作加密與認證，如此可以降低惡意的攻擊；及使用新制訂的 IDMEF 格式作為不同入侵偵測系統間訊息傳遞的標準交換格式。

五、計畫成果自評

本計畫所提的聯合防禦入侵偵測機制，每個節點具有入侵偵測與入侵反應機制，因此，每個節點本身即可進行入侵阻擋的防禦工作。另外可透過溝通模組的警告分類與門檻值的設定，以降低誤判率及因聯合防禦機制所產生的網路執行效率問題；另外，每個節點並非完全接受其他節點送來的警告訊息，因為我們透過多數決機制來決定是否要接受此警告訊息。因此，本研究機制應可提供在此環境下，提供第二道安全且有效率的防線。

參考文獻

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

[2] D.J. Ragsdale, C.A. Carver, Jr. J.W. Humphries, U.W. Pooch, “Adaptation techniques for intrusion detection and intrusion response systems,” 2000 IEEE International Conference on Systems, Man, and Cybernetics, Vol.4 , 8-11 Oct. 2000 p.2344-p.2349.

[3] E.H, Spafford and D. Zamboni, “Intrusion Detection Using Autonomous Agent,” Computer Networks, vol.34, issues 4, p.547-p.570, 2000.

[4] H. Deng, W. Li and D.P. Agrawal, “Routing Security in Wireless Ad Hoc Networks,” IEEE Communications Magazine, Vol. 40, Issue 10, October 2002, p.70-p.75.

[5] J. Kong, P. Zerfos, H. Luo, S. Lu and L. Zhang, “Providing Robust and Ubiquitous Security Support for Mobile Ad-Hoc Networks,” IEEE 9th International Conference on Network Protocols (ICNP'01), 2001.

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

[7] L. Zhou and Z. Haas, “Securing Ad Hoc Networks,” IEEE Network , pp.24-30, Dec, 1999.

[8] 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.

[9] S.R. Snapp, J. Brentano, G.V. Dias, T.L. Goan, T. Grance, L.T. Heberlein, C.L. Ho, K.N. Levitt, B. Mukherjee, D.L. Mansur, K.L. Pon, and S.E. Smaha, “A system for distributed intrusion detection,” Compcon Spring’91, Feb-March 1991, p.170-p.176.

[10] R. Martin, “Snort – Light Weight Intrusion Detection for Networks,” http://www.snort.org

[11] 顧吉宇，”一個針對無基礎行動網路的聯合式的入侵偵測機制” 國立交通大學資訊管理研究所碩士論文，民 92。