應用在無線感測網路上的智慧型混合式入侵偵測系統

嚴國慶
朝陽科技大學
企管系
kqyan@cyut.edu.tw

王淑卿*
朝陽科技大學
資管系(聯絡人)
scwang@cyut.edu.tw

王順生
朝陽科技大學
工管系
sswang@cyut.edu.tw

劉佳瑋
朝陽科技大學
資管系
s9614640@cyut.edu.tw

摘要

隨著無線感測網路(Wireless Sensor Networks：WSNs)的發展，WSNs 的應用愈來愈受到重視，因此安全性的議題也日趨重要。由於感測器(Sensor)是由一種便宜又小的裝置所組成，且通常被部署於一個公開且未受到保護的環境下，所以極易遭受敵人的入侵與攻擊。又由於在 WSNs 的拓樸下，資料搜集中心(Sink)具有強大的資源且不受電力的限制，因此在本研究中，提出一套建置在資料搜集中心的入侵偵測系統(Intrusion Detection System：IDS)。本研究所提出的 IDS，是一套智慧型混合式入侵偵測系統(Hybrid Intrusion Detection System：HIDS)，結合了異常(Anomaly)偵測與誤用(Misuse)偵測兩種模式。研究中藉由異常偵測的高偵測率和誤用偵測的高準確性，目的是希望達到高偵測率及低誤判率的目標。異常偵測模式採用規則式分析的技術來建立正常的行為模式。誤用偵測模式則採用自適應共振理論網路(Adaptive Resonance Theory Network：ART)來將攻擊行為進行分類，由於 ART 屬於非監督式學習的方式，因此能夠學習新型的攻擊行為，以達到智慧型偵測的目的。

關鍵詞： 無線感測網路、混合式入侵偵測系統、異常偵測、誤用偵測

Abstract

Recent advances in Wireless Sensor Networks (WSNs) make them more important to apply. Therefore, security issues are more significant in WSNs. WSNs are susceptible to some types of attacks since they are consisted of cheap and small devices and are deployed in open and unprotected environments. In this research, an Intrusion Detection System (IDS) created in sink is proposed. The proposed IDS is an intelligent Hybrid Intrusion Detection System (HIDS). It consists of anomaly model and misuse model. The goal is to raise the detection rate and lower the false positive rate by the advantages of misuse detection and anomaly detection. The rule-based analysis method is used to the anomaly detection model. In addition, the Adaptive Resonance Theory Network (ART) is adopted to the misuse detection model. However, ART is an unsupervised learning method, and it can learn the new attack behavior to achieve the goal of intelligent detection.

Keywords: Wireless sensor network, Hybrid IDS, Anomaly detection, Misuse detection

1. 前言

由於無線通訊及微型製造技術的進步，設計出體積小、成本低及耗電低的感測器，具有感應、計算以及通訊的能力。因此近年來無線感測網路(Wireless Sensor Networks：WSNs)的議題不斷地被專家學者所關切。WSNs 是一種無基礎建設(Non-infrastructure)的網路型態，透過大量部署的感測節點(Sensor Node)形成一個感測網路。然因感測節點電力有限，為了減少感測器在傳輸上的電力消耗，無線感測網路利用多重跳躍(Multi-hop)的方式來建立網路的路由繞徑，再將資料經由多個感測器所組成的路徑傳回基地台[5]。

無線感測網路是一種以任務為導向的應用網路型態，其最大的致命傷就是有限的資源。因為硬體設計上的考量，使其受到許多限制(如：計算能力、記憶體、電力消耗…等)，讓整個無線感測網路的設計需要更為嚴謹，其中又以電力消耗為首要考量因素。因此，為了提昇整個網路的生命週期，提供一個有效節省電力的網路架構以降低其電力消耗，是設計無線感測網路時是一個重要的關鍵因素之一。

無線感測網路主要的功能是資訊的蒐集與監控，透過大量部署的感測節點來偵測週遭環境或是特定目標，進而將收集到的資訊以無線傳輸的方式回傳給網路監控者，並分析這些資訊來瞭解實際的狀況。因此其應用的範疇相當廣泛，涵蓋了商業、軍事、健康與環境等諸多方面。

由於無線感測網路是由許多成本低及體積小的裝置所組成，且被部署於一個未受保護的環境下，因此極容易受到入侵與攻擊。預防機制可以保護無線感測網路來對抗一些攻擊，然而有一些攻擊卻沒有已知的預防方法，而且預防機制並不能夠保證一定能阻擋入侵者，對於這些特例，必須要有一套入侵偵測的機制來應對，入侵偵測系統(Intrusion Detection System：IDS)除了偵測入侵之外，還可以取得攻擊技巧的相關資訊來幫助發展預防系統。

入侵偵測系統猶如網路監控者及警報裝置，能在入侵行為造成危害前即時發出警訊以進行相關反應措施，防範系統遭致破壞。一般入侵偵測模式，依據其偵測模式，可歸類為兩大類 [1]：一種為異常偵測(Anomaly Detection)，建立一個正常的行為模式，將所偵測到的現行行為與正常行為模式進行比較，若差異甚大則視為異常行為。優點是偵測率高，但正確率不高，容易將正常行為視為異常的攻擊。而另一種為誤用偵測(Misuse detection)，利用已知的攻擊來建立各種攻擊模式，再與所偵測到的現行行為進行比較，但它無法偵測新型的攻擊，若現行攻擊行為不存在於模式庫中，即無法偵測此行為。

入侵偵測系統的最終目標是希望能夠達到高的偵測率及低的誤判率，而目前市面上的商業產品大都是以「特徵比對」的技術為基礎。但利用「特徵比對」技術只能偵測已知的攻擊，卻無法偵測新型的攻擊。然而，在這個充滿變數的環境中，雖然使用誤用偵測的正確性很高，但倘若只使用誤用偵測是不夠的。因此，為了偵測新型的攻擊，管理者必須手動去更新建立好的模式庫。因此，在本研究所建置的智慧型混合式入侵偵測系統中，除了透過誤用偵測技術偵測異常的行為外，亦加入異常偵測的技術偵測新型的攻擊，藉由異常偵測的高偵測率和誤用偵測的高準確性，達到高偵測率及低誤判率的目標。

目前大多數有關無線感測網路的入侵偵測系統的研究，都是將入侵偵測系統建置在感測節點上[7,10]。但由於一般的感測節點都有資源限制的問題，使得運算量大及耗電量大的技術無法被實作。由於在無線感測網路的實際應用中，每個節點所感測到的資料，最後都必須經由資料搜集中心來進行資料融集(Data Aggregation)。因此，在本研究中將入侵偵測系統應用在資料搜集中心上，利用其強大的資源，開發一套智慧型偵測系統，使過去在感測節點上無法實作的技術能夠實現。

在本研究中，提出在資料搜集中心上開發一套智慧型混合式入侵偵測系統，結合了異常偵測與誤用偵測兩種模式。藉由異常偵測的高偵測率和誤用偵測的高準確性，目的是希望達到高偵測率及低誤判率的目標。而由於攻擊行為將隨著使用者使用行為的成長，及資訊技術的進步，以致攻擊總類不斷地推陳出新，若未能持續改善系統的能力，既有的 IDS 將無法提供系統的安全防護。因此，為了解決這個問題，本研究所提出的入侵偵測系統必須為智慧型的偵測，使系統遭遇到新型的攻擊行為時，能夠及時發現並學習以產生新偵測的類別。異常偵測模式是藉由訓練正常的行為模式來偵測現行行為是否異常，本研究採用規則式(Rule-based)分析的技術來建立此正常行為模式。誤用偵測模式是利用事先定義好的攻擊模式來判定是否為攻擊行為，本研究採用自適應共振理論網路(Adaptive Resonance Theory Network, ART)來將攻擊行為進行分類，由於其屬於非監督式學習的方式，因此能夠學習新型的攻擊行為，以達到智慧型偵測的目的。

在本文中，第二節將說明在無線感測網路上常見的攻擊行為及本研究所採用的入侵偵測分析工具。第三節將說明本研究所提出的方法與架構。第四節則說明結論與未來工作。

2. 文獻探討

在本節中，將說明在無線感測網路上常見的攻擊行為及本研究所採用的入侵偵測分析工具。

2.1 無線感測網路的攻擊行為

由於無線感測網路是由許多成本低及體積小的裝置所組成，且被部署於一個未受保護的環境下，因此是容易遭受到攻擊的。由過去在無線感測網路上的攻擊行為的相關研究分析[12]，可知依據入侵者的目的不同，攻擊行為可分成兩類：(1)透過各種管道來更改路由資

訊，破壞感測網路的連線，使整體網路陷入混亂；(2)透過不斷地重送或傳送大量無意義的封包，耗盡感測網路的連結頻寬以及感測節點的電力以癱瘓整個網路。

依據攻擊行為的類別，首先分析無線感測網路中常見的攻擊行為，找出這些攻擊行為的特性，並將其分類。以下說明在無線感測網路上常見的八種攻擊行為：[9,13,14]

(1) Spoofed、Altered、或 Replayed Routing Information：攻擊者透過欺騙、更改或重送路由資訊，讓其它節點把攻擊者當作是目的地節點且傳回它們所感測的資料。主要是用來混淆路由資訊，當所感測的資料藉由這個假冒的節點進行傳送時，這些感測的資料可能會被丟棄、竄改或複製。

(2) Select Forward：攻擊者會選擇性的轉送收到的封包或是直接丟棄，使封包無法正確到達目的地，導致網路陷入混亂狀態。當攻擊者位於封包傳輸路徑上時，該攻擊通常是最有效的。此攻擊的另一種特殊型式是 black hole 攻擊，攻擊者拒絕轉送它收到的每一個封包，使進入此節點的封包都陷入黑洞。

(3) Sinkhole：攻擊者聲稱自己是電力充足、性能可靠且具有高效能的節點，從而吸引周圍的節點選擇此節點作為資料傳輸路徑中的節點。一旦資料都經過此妥協節點時，攻擊者就可以獲得這些資料，而真正該收到資料的節點則無法正常的接收資料。因此，無線感測網路對 Sinkhole 攻擊特別敏感。

(4) Sybil Attack：攻擊者不斷地聲明其有多重身份，使得它在其它節點前具有多個不同的身份。Sybil Attack 對地理路由協定構成很大的威脅，因為地理路由協定是假設節點能夠知道自身的地理位置或者透過標竿節點的位置來計算自身的位置。該路由協定中，節點之間的數據通訊常常需要知道鄰居節點的位置訊息，當該路由協定受到 Sybil Attack 時，一個節點可以偽造多個地址，達到攻擊的目的。

(5) Wormholes：Wormholes 攻擊通常需要兩個攻擊者相互串通，合謀進行攻擊。典型的 Wormholes 攻擊是一個攻擊者在資料搜集中心附近，另一個攻擊者在離資料搜集中心較遠的地方，較遠的節點聲稱自己和資料搜集中心附近的節點可以建立低延遲、高頻寬的連結，從而吸引周圍節點將其封包發送到此節點。

(6) Denial of Service：攻擊者在一段期間內傳送大量且密集的封包至特定節點，來消耗該節點的電力，以致造成被攻擊節點癱瘓。Denial of Service 也可以同時透過多個攻擊者來發動此攻擊，這樣的攻擊又更難以防禦，且傷害程度又更大。

(7) Hello Floods：由於很多路由協定都需要感測節點定時發送 Hello 訊息，聲明自己是周圍節點的鄰近節點，但當一個電力較強的攻擊者以足夠大的功率廣播 Hello 訊息時，收到 Hello 訊息的節點會誤以為這個攻擊者是它們的鄰近節點，在往後資料傳輸的過程中，很可能會選擇這個攻擊者當作傳輸的路徑，而向攻擊者發送封包。而事實上，該節點離攻擊者距離可能較遠，以普通的發射功率傳輸的封包根本到不了目的地。

(8) Acknowledgment Spoofing：攻擊者的目的是使發送者相信一條差的連結是好的，或一個已死的節點是活著的。例如，發送者向某鄰居節點發送封包，當攻擊者監聽到該鄰居節點處於「死」的狀態時，冒充該鄰居節點向發送者回覆一個確認訊息，發送者誤以為該節點處於「活」的狀態，造成發送到該鄰居節點的資料之遺失。

經由八種攻擊行為的說明後，可依據攻擊名稱、攻擊行為、攻擊數量、及影響範圍將在無線感測網路上常見的攻擊行為表列於表 1 中。由表 1 的資料得知大部份的攻擊行為都是透過不正當的路由更新，以致影響資料的傳輸。而由於在無線感測網路上所進行的應用，大都是藉由感測節點感測並收集資料，接著傳送到資料收集中心進行資料融集，以及後續的相關工作。因此，在資料收集中心探討入侵偵測系統，確有其必要性。

2.2 入侵偵測分析工具

由於分析工具的選取是影響入侵偵測效能最主要的因素之一，因此為了建置一個智慧型混合式入侵偵測系統，合適工具的選擇是一個非常重要的工作[1]。所以在本節中，將先說明本研究所使用的分析工具。

表 1、在無線感測網路上常見的攻擊行為

攻擊名稱	攻擊行為	攻擊數量	影響範圍
Spoofed、Altered、Replayed routing information	不正當的路由更新	單一	局部區域
Select forward	不正當的資料傳遞	單一	局部區域
Sinkhole	不正當的路由更新	單一	局部區域或整體網路
Sybil	不正當的路由更新	單一	局部區域或整體網路
Wormholes	不正當的路由更新	多個	局部區域
Denial of Service	不正當的資料傳遞	單一或多個	整體網路
Hello floods	不正當的路由更新	單一	整體網路
Acknowledgment spoofing	不正當的路由更新	單一	局部區域

Qiao 等學者曾整合誤用偵測及異常偵測，提出混合的偵測方式，利用誤用偵測的高正確性去偵測舊的入侵行為，再用異常偵測來偵測新型的攻擊，以達到在低誤判率的前提下接近百分之百的偵測率[11]。在 Depren 等學者的研究中，提出的混合式入侵偵測系統，除結合了誤用偵測與異常偵測的模式，再利用決策支援系統來整合兩個模式的偵測結果，以達到高偵測率及低誤判率[8]。

然而過去的相關研究，針對新型的攻擊行為發生時，無法及時發現並進行偵測。因此，為了解決這個問題，本研究所提出的混合式入侵偵測系統必須為智慧型的偵測，使其遭遇到新型的攻擊行為時，能夠及時發現並學習這些攻擊行為的特徵，以建立新的攻擊類別。異常偵測模式是藉由訓練正常的行為模式來偵測現行行為是否異常，本研究採用規則式(Rule-based)分析的技術來建立此正常行為模式。誤用偵測模式是利用事先定義好的攻擊模式來判定是否為攻擊行為，本研究採用自適應共振理論網路(Adaptive Resonance Theory Network, ART)將攻擊行為進行分類。由於 ART 屬於非監督式學習的方式，因此能夠學習新型的攻擊行為，以達到智慧型偵測的目的。

2.2.1 規則式分析 (Rule-based Analysis) [4]

有許多領域的知識需要具備推論的特性，例如：醫生依據病人的症狀來推論其可能罹患的疾病。而因為人類的思考極為複雜，以致於許多知識難以用演算法來表示，因此可以利用規則式分析的方式來表示。規則式分析主要用來表現專家的思考模式，藉由專家的經驗及觀察來定義對應的規則，而最基本的規則型式為「若…則」(if…then)分析的方式，亦即如果「狀態」成立則獲得「結論」。而根據建立規則的方式可把規則式分析方法分成兩類：

(1) 向前鏈結(Forward Chaining)：又稱為「資料驅動」的推論方式，此種方法是從「原因」往「結果」的方向推演，例如：若「流鼻水」則「感冒」了。此法的優點是所推出的結論較為準確，誤判率低，但是缺點就是無法推測新的事件。

(2) 向後鏈結(Backward Chaining)：又稱為「目標驅動」的推論方式，此種方法是由「結果」去推測可能發生的「原因」，例如：若「感冒」則可能發生「流鼻水」或「咳嗽」的症狀。此法可以推測出所有可能的原因，但缺點是其誤判率高。

本研究將向前鏈結規則式分析方法應用在異常偵測上，以規則的方式來描述事件，並將「原因」存放於規則庫中，然後將現行的行為與規則庫中的規則進行比對，藉以判斷是否為異常的行為。

2.2.2 自適應共振理論網路

自適應共振理論網路 (Adaptive Resonance Theory Network：ART)是在 1976 年，由 Grossberg 所提出[6]，是一種非監督式學習網路模式。其基本的精神是由問題領域取得只有輸入變數值的訓練範例，並從中學習內在的群集規則，用以推論新資料屬於何種群集，若是該筆資料與現有群集結果不合時，則產生一個新群集。ART 具有下列特性[2]：

(1)穩定性與可塑性

由於 ART 具有穩定性，所以在處理的過程

中若遇到不相關的資訊輸入系統時，系統將會與現有的資訊比較，若已有類似的資訊則不會改變其群集結果。又因具有可塑性，故當輸入資訊與現有資訊夠相似或具有密切相關性時，系統便可迅速的進行學習並納入記憶，具有線上學習的能力，即可邊作邊學習。

(2)非監督式學習

由於非監督式學習能夠直接從問題領域中取得訓練範例，因此在不知道其輸出結果的情況下即可進行學習，從中學習範例內在的群集規則，以應用在新的案例上。而 ART 便是一種非監督式學習的網路模式，故在學習過程中並不需要訓練範例的相對目標值，即可進行學習，因網路本身就有能力對輸入的資訊進行學習與取捨。

(3)快速學習能力

由於一般監督式學習的網路模式，容易受到輸入層、輸出層及隱藏層數目的多寡而影響整體的學習速率，也就是說監督式學習網路，必須提供足夠的訓練範例給網路進行學習，經由學習不斷地調整輸入、輸出以及隱藏層之間的權重值，以應用於未來輸入向量分析之用。而 ART 的學習方式則是當訓練範例輸入後，便立即進行學習並進行群集分析，所以此類模式除了可以直接在線上學習外，更可達到快速學習的目的。

由於建置智慧型混合式入侵偵測系統，必須使用一個能夠處理大量資訊的方法，此方法除了能夠維持整體的穩定性外，且為了因應不斷改變的攻擊行為，所以需要具有線上學習的能力，而 ART 即可應付上述狀況。為了達成智慧型混合式入侵偵測系統的目標，在本研究中，將 ART 應用在入侵偵測系統上，除了能夠由偵測環境中自動取得訓練資料外，並能學習資料中內在的群集規則，將正常行為與攻擊行為區分出來，且透過警戒值測試進行判定，以及時發現新型的攻擊行為。

圖 1 為 ART 的網路架構，是由輸入層、輸出層及其網路連結所組成[3]。

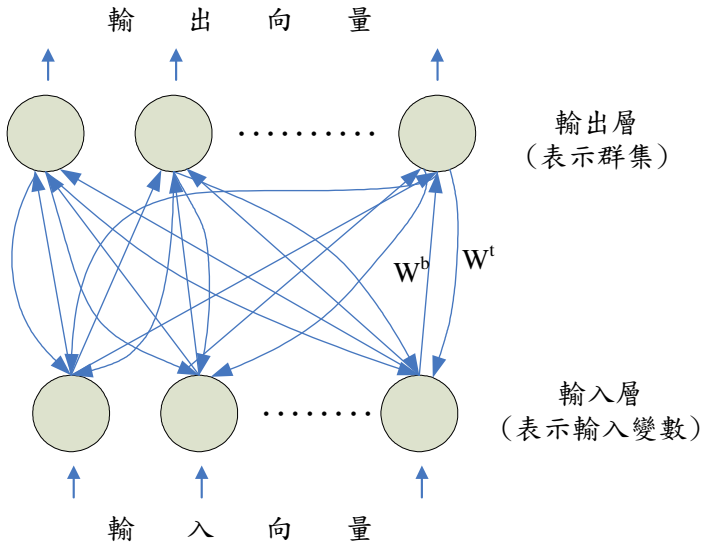

圖 1、ART 網路架構

輸入層：表示網路的輸入變數，即訓練範例的輸入向量，或稱特徵向量，其處理單元的數目則依據問題領域而定。

輸出層：表示網路的輸出變數，即訓練範例的群集，其處理單元的數目在學習之初時只有一個，隨著學習的過程中會逐漸增加，而最後會穩定在一定的數目，學習過程即結束。

網路連結：各輸入層單元與輸出層單元之間都有二條網路連結：

(1) 由下而上的加權值為 W^b，是用來計算範例的輸入向量對一輸出層處理單元的「匹配值」之用，而匹配值最高的輸出層處理單元會優先被選來做「警戒值測試」，其中 W^b 的值為[0,1]的連續值。

(2) 由上而下的加權值為 W^t，是用來計算範例的輸入向量對一輸出層處理單元的「相似值」之用，而「相似值」是用來判定一輸出層處理單元是否通過「警戒值測試」，其中 W^t 的值為{0,1}的二元值。

ART 的運作模式為每個輸出層的處理單元各代表一個群集，而輸入層的每個處理單元則共同對應到一筆輸入向量，其透過「警戒值測試」的方法來判定這筆輸入向量是否屬於此群集。然而，能夠通過警戒值測試的輸出層處理單元可能不只有一個，因此 ART 便以「匹配值」來做為其判斷的基準，依各輸出層處理單元的匹配值高低，從匹配值最高的處理單元到匹配值最低的處理單元逐一做警戒值測試。

在 ART 的架構中，有一個重要的參數需要由使用者自訂，也就是警戒值 (Vigilance Value)，其所扮演的角色為控制新的輸入向量與現有群集的契合度，警戒值越高，輸出層處理單元就越不容易通過警戒值測試，因此越需要產生新的群集，故輸出層處理單元的數目較多。反之，警戒值越低，輸出層處理單元就越容易通過警戒值測試，因此不需要產生新的群集，輸出層處理單元的數目也較少。

3.研究方法與架構

因為資料搜集中心擁有豐富的資源，因此本研究提出一套建置在資料搜集中心的智慧型混合式入侵偵測系統，能夠將原本在感測節點上無法做到的技術實現。本研究結合了異常偵測與誤用偵測兩種模式，以進行入侵偵測，透過混合使用的方式來同時保有兩種模式的優點，透過異常偵測模式的高偵測率來偵測攻擊行為，誤用偵測模式的高正確性來降低誤判。

本研究使用異常偵測模式來做為第一道的偵測防線，主要是利用它來篩選攻擊或非攻擊的行為。由於無線感測網路環境中所需偵測的封包數量龐大，而且絕大多數的封包都是正常的，只有少數的封包為攻擊行為，因此本研究的異常偵測系統所扮演的角色就像一個過濾器，將經過的封包先進行篩選，被判定為異常者再經由誤用偵測模式來做更進一步地偵測。

由於異常偵測模式在判斷是否為攻擊行為的依據是利用正常的行為模式，因此只要現行行為與此正常行為模式有所差異，系統就會判定為異常，所以經常會將正常的通訊判定為異常的情況，而造成誤判的問題。但因異常偵測模式具有「寧可錯殺一萬，也不可放過萬一」的特性，所以不會將異常的通訊判定為正常的。因此，在本研究中首先以異常偵測模式來過濾大量的封包，當整體資訊量降低後，再經由誤用偵測模式來進行偵測。換言之，透過本研究所提出的異常偵測模式的篩選過程，可排除掉大量正常的封包，以避免誤用偵測模式偵測這些正常封包所浪費的資源。

在本研究中，誤用偵測模式主要是用來進行更深一步地偵測，扮演第二道偵測防線。其作法是將異常偵測模式判定為異常的封包，再透過誤用偵測模式進行第二次的偵測，以檢查異常偵測模式是否誤判，並分類出誤用的種類，以提供系統工程師進行後續的處理。而在本研究中，則使用具有非監督式學習能力的 ART，因 ART 能夠從環境中所取得的資料找出內在的群集規則，使得誤用偵測模式具有線上學習的能力，能夠偵測新型的攻擊行為，因此能夠達到智慧型偵測的目的。

圖 2 所示為本研究所提出的智慧型混合式入侵偵測系統的架構，將所有聚集到資料搜集中心的封包記錄輸入至系統中，利用異常偵測模式先將封包紀錄進行篩選，以降低整體資訊量，再將被判定為異常的封包輸入至誤用偵測模式中，透過前置處理將封包記錄轉換成 ART 可辨識的資料型態，再經由 ART 判定是否為入侵行為，若是，則回報管理者為何種入侵行為。

3.1 異常偵測模式

異常偵測是先建立一個正常的行為模式，接著將所偵測到的現行行為與現存模式進行比較，若差異甚大則視為異常行為。而在無線感測網路的環境中，主要監控的是封包的狀態，因此必須為封包建立一個正常的行為模式，本研究採用規則式分析的方法來建立我們的異常偵測模式。

本研究所建立的異常偵測模式，其流程如圖 3 所示。建立異常偵測模式之流程可分為四個步驟：

Step 1： **分析無線感測網路上過去所傳送封包的歷史紀錄。**蒐集過去在無線感測網路上進行通訊的封包，將封包分為正常與異常兩類，藉以提供挑選影響封包正常或異常的關鍵屬性。

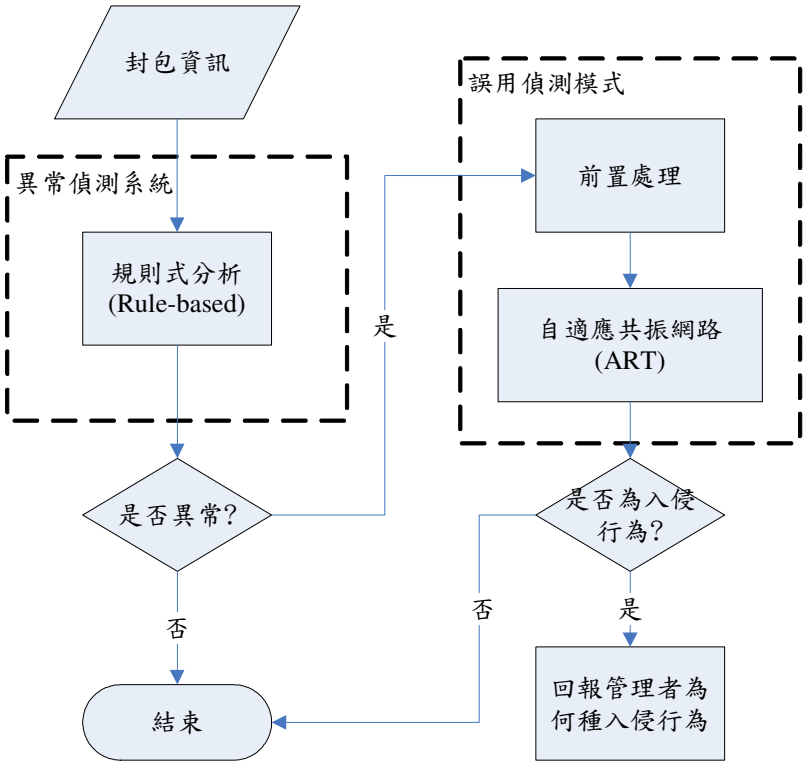

圖 2、系統架構

Step 2： **特徵挑選。**將正常和異常的封包進行比較，找出區分封包正常或異常的關鍵特徵，以協助本研究建立異常偵測規則。

Step 3： **建立異常偵測規則。**依據定義為正常的封包及挑選的屬性來建立規則，並將建立好的規則存放於規則庫中。

Step 4： **建立正常行為模式。**所建立的規則庫即為正常行為模式，往後即依據此模式與輸入的封包進行比對。

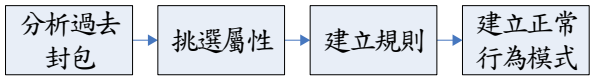

圖 3、建立異常偵測模式之流程

在無線感測網路中，當所有的感測節點與資料搜集中心進行通訊的時候，所有經過的封包都必須透過異常偵測模式的偵測，當經過的封包符合正常行為模式時，則判定其為正常的封包。反之，則判定其為異常封包，並轉送至誤用偵測模式進行第二階段的偵測，異常偵測模式偵測流程如圖 4 所示。

3.2 誤用偵測模式

由於誤用偵測模式是利用已知的攻擊行為來建立各種攻擊模式，再與偵測到的現行行為進行比較，因此必須建立一個攻擊行為的模式庫。由於攻擊行為會不斷地推陳出新，因此本研究需具備線上學習的能力，以持續改善系統的能力，故研究中使用具有非監督式學習能力的 ART 來進行訓練，以建立本研究的誤用偵測模式。

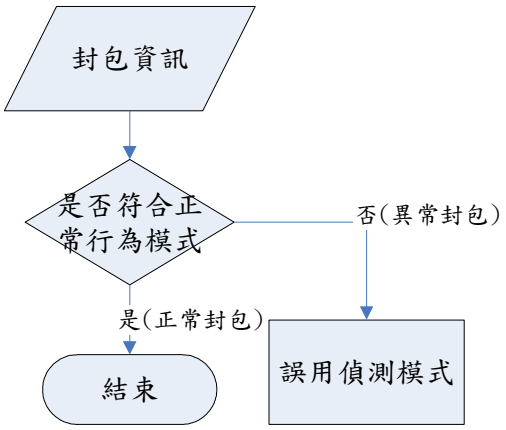

圖 4、異常偵測模式偵測流程

圖 5 為本研究的誤用偵測模式架構，架構是由輸入層、輸出層和其網路連結所組成。輸入層的輸入向量是經由異常偵測模式判定為異常的封包，轉送到誤用偵測模式來做更進一步的偵測，而其處理單元的數目則依據分析封包所挑選的特徵項目而定。輸出層的每個處理單元各代表一個群集，而這些群集基本上會有二種狀態，包括「正常模式」與「攻擊模式」。由於經過整理分析後，在無線感測網路上可能遭遇的攻擊行為可分為八種，包括：Spoofed，Altered，或 Replayed Routing Information、Select Forward、Sinkhole、Sybil、Wormholes、Denial of Service、Hello Floods、及 Acknowledgment Spoofing。因此，經過 ART 訓練學習後，會將所有的誤用群集歸類為八個攻擊模式與一個正常模式。

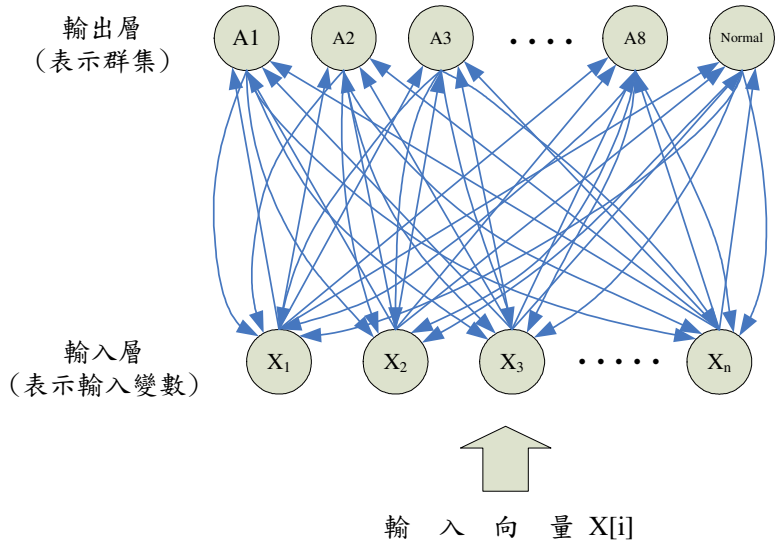

圖 5、誤用偵測模式架構

而為了判斷新產生的群集屬於「正常模式」或是「攻擊模式」的狀態，本研究加入一個「不確定模式」狀態來輔助判斷，將新產生的群集都先歸類成「不確定模式」的狀態，最後依據

其成員數的多寡來判定其屬於正常或攻擊模式。因為在通訊的過程當中，絕大多數的封包都是正常的，遭受攻擊的封包只佔傳送封包的少數，因此可以設一個門檻值，若其成員數高於門檻值則判定此群集為正常，並將其歸類到正常模式中。反之，若低於門檻值則判定此群集為攻擊，也就是產生一個新的攻擊模式。目的是希望讓整個系統能夠更加嚴謹，透過觀察其成員數的多寡來決定其屬於正常或攻擊模式。

本研究所提出的誤用偵測模式偵測流程如圖 6 所示，一個被判定為異常的封包在進入誤用偵測模式之前，必須先進行前置處理的工作，也就是將封包內容轉換成二元值，然後再輸入至系統中，再來計算這個封包對應到每一個群集的「匹配值」，接著挑選匹配值最高者，來計算其「相似值」並進行「警戒值測試」。如果封包通過警戒值測試，則這個封包即屬於此群集，只需修改加權值即可。

反之，若封包未能通過警戒值測試，則這個封包就不屬於此群集，必須再找是否還有可用之群集，若有，則一樣挑出匹配值最高者，計算出它的相似值及做警戒值測試，直到找出符合這個封包的群集為止。但若所有的群集都比對完之後，還是沒有找到對應的群集的話，則產生一個新的群集。因此，本研究所提出的誤用偵測模式除了能夠將被誤判的封包排除，還能夠學習新型的攻擊行為，達到在進行偵測的同時，也能透過學習的機制獲得新型攻擊行為的資訊。

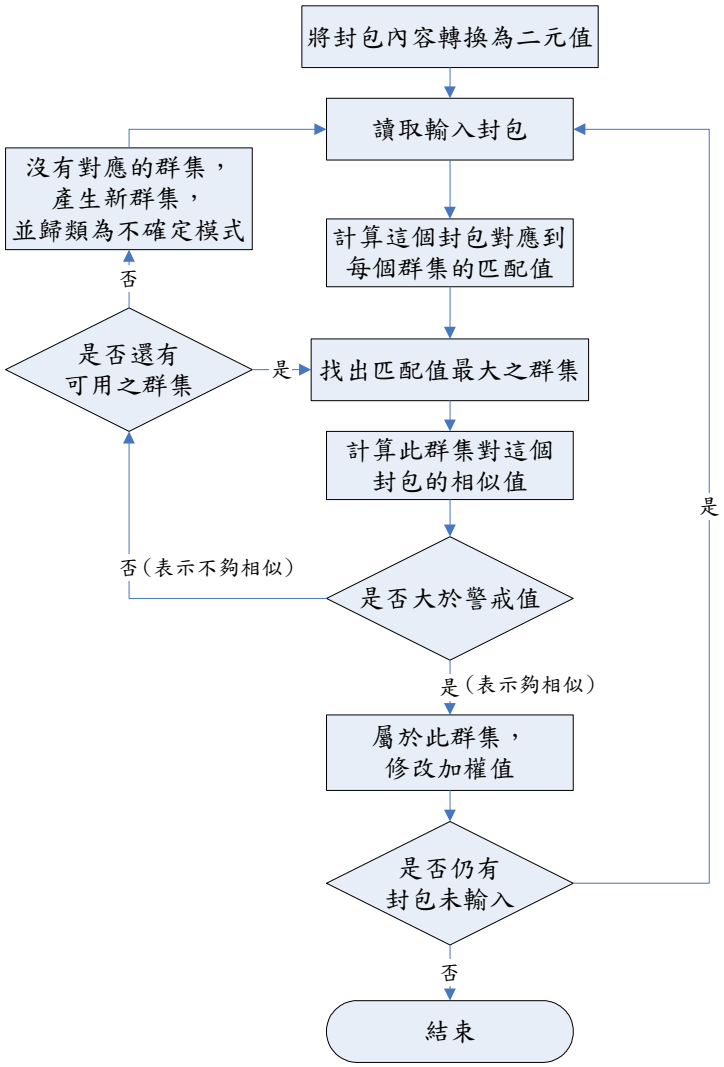

圖 6、誤用偵測模式偵測流程

4. 結論與未來工作

在本研究中，將入侵偵測系統建置在無線感測網路的資料搜集中心上，利用其強大的資源，開發一套智慧型混合式偵測系統。此智慧型混合式偵測系統結合了異常偵測與誤用偵測兩種模式，透過異常偵測模式來過濾大量的封包資訊，誤用偵測模式來將被判為異常的封包做更進一步地偵測。然而，由於攻擊行為會不斷地推陳出新，因此入侵偵測系統需具備線上學習的能力，以持續改善系統的能力，故本研究使用具備非監督式學習能力的 ART 來建立本研究的誤用偵測模式，以達到智慧型偵測的目的。

由於誤用偵測模式中有兩個重要的參數需要定義，包括警戒值與判定不確定模式的門檻值，因此在未來的研究中，將透過模擬的方式來找出合適的值。

除此之外，由於無線感測網路是由許多感測節點所構成，然而感測節點卻常受硬體資源的限制，而以階層式架構建置其網路拓樸。然而在階層式網路拓樸中，又以叢集頭(Cluster Head)最常遭受入侵與攻擊。因此在未來的研究中將著眼在透過叢集頭進行入侵偵測，除節省整體網路的電力消耗，並且能有效降低了整體網路的資訊量，以延長整個網路的生命週期為目的。

參考文獻

[1] 李駿偉，***入侵偵測系統分析方法效能之定量評估***，中原大學資訊工程系碩士論文，桃園，2002。

[2] 傅心家，***神經網路導論***，定碁科技股份有限公司，台北，1991。

[3] 葉怡成，***類神經網路模式應用與實作***，儒林出版社，台北，2003。

[4] 曾憲雄、黃國禎，***人工智慧與專家系統: 理論・實務・應用***，旗標出版股份有限公司，台北，2005。

[5] Akyildiz, I. F., Weilian, S., Sankarasubramaniam, Y., and Cayirci, E., "A Survey on Sensor Networks," ***IEEE Communications Magazine***, Vol. 40, No. 8, pp. 102-114, 2002.

[6] Carpenter, G. A. and Grossberg, S., "The ART of Adaptive Pattern Recognition by a Self-organizing Neural Network," ***IEEE Computer***, Vol. 21, Issue 3, pp. 77-88, 1988.

[7] Da silva, A. P. R., Martins, M. H. T., Rocha, B. P. S., Loureiro, A. A. F., Ruiz, L. B., and Wong, H. C., "Decentralized Intrusion Detection in Wireless Sensor Networks," ***Proceedings of the 1st ACM International Workshop on Quality of Service & Security in Wireless and Mobile Networks***, pp. 16-23, 2005.

[8] Depren, O., Topallar, M., Anarim, E., and Ciliz, M. K., "An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks," ***Expert Systems with Applications***, Vol. 29, Issue 4, pp. 713-722, November 2005.

[9] Karlof, C. and Wagner, D., "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," ***Ad Hoc Networks***, Vol. 1, Issues 2-3, pp. 293-315, September 2003.

[10] Onat, I., and Miri, A., "An Intrusion Detection System for Wireless Sensor Networks," ***IEEE International Conference on Wireless and Mobile Computing, Networking and Communications***, Vol. 3, pp.253-259, Aug 2005.

[11] Qiao, Y. and Weixin, X., "A network IDS with low false positive rate," ***Proceedings of the 2002 Congress on Evolutionary Computation***, Vol. 2, pp. 1121-1126, May 2002.

[12] Su, W. T., Chang, K. M., and Kuo, Y. H., "eHIP: An Energy-efficient Hybrid Intrusion Prohibition System for Cluster-based Wireless Sensor Networks," ***Computer Networks***, Vol. 51, Issue 4, pp. 1151-1168, March 2007.

[13] Wang, Y., Attebury, G., and Ramamurthy, B., "A Survey of Security Issues in Wireless Sensor Networks," ***IEEE Communications Surveys & Tutorials***, Vol. 8, No. 2, pp. 2-23, Second Quarter 2006.

[14] Wood, A. D. and Stankovic, J. A., "Denial of Service in Sensor Networks," ***Computer***, Vol. 35, Issue 10, pp. 54-62, Oct 2002.