Regular Paper

Communications of the CCISA
Vol. 25 No. 1 Feb. 2019

一個混合式的分類演算法應用於入侵偵測系統

陳則宏 [1,a]、陳羿霖 [1,b]、張維晏 [1,c]、蔡崇煒 [2,d*]
[1] 國立中興大學 資訊科學與工程學系、[2] 國立中山大學 資訊工程學系
[a] enter201249@gmail.com、[b] a0989735018@gmail.com、[c] keoinn@gmail.com
[d] cwtsai@mail.cse.nsysu.edu.tw

摘要

入侵偵測系統可以被視為網路管理系統中，用於檢查與警示異常網路行為之子系統。隨著網際網路發展以及網路架構複雜程度增加，許多不同的攻擊方式因此而產生。傳統的入侵偵測系統，無法有效地偵測出這些攻擊，因此本研究提出一個混合式的分類演算法應用於入侵偵測系統，提高系統判斷異常攻擊行為的準確度，並減少分類演算法的計算時間。這個方法結合 *k*-means 分群演算法、支持向量機分類演算法以及搜尋經濟學超啟發式演算法。實驗結果說明利用這個混合式的策略，可以讓入侵偵測系統在較複雜的網路攻擊分類問題上，提供較高的準確度。

關鍵詞：入侵偵測系統、分類演算法、超啟發式演算法。

A Hybrid Classification Algorithm for Intrusion Detection System

Ze-Hong Chen[1, a], Yi-Lin Chen[1,b], Wei-Yan Chang[1,c], and Chun-Wei Tsai[2,d*]
[1]Computer Science and Engineering, National Chung Hsing University, Taiwan, R.O.C.
[2]Computer Science and Engineering, National Sun Yat-sen University, Taiwan, R.O.C.
[a]enter201249@gmail.com, [b]a0989735018@gmail.com, [c] keoinn@gmail.com,
[d] cwtsai@mail.cse.nsysu.edu.tw

Abstract

An intrusion detection system (IDS), which can be regarded as a subsystem of a network management system, plays the role of detecting and preventing abnormal network behaviors. With the advance of the Internet and the increase of the complexity of network architectures, many attack methods have been developed. However, most traditional intrusion detection systems are incapable of recognizing these attacks. Therefore, this study will present a hybrid classification algorithm for an intrusion detection system to improve its accuracy rate and reduce its computation time. The proposed algorithm integrates k-means (a clustering algorithm), support vector machine (a classification algorithm), and search economic (a

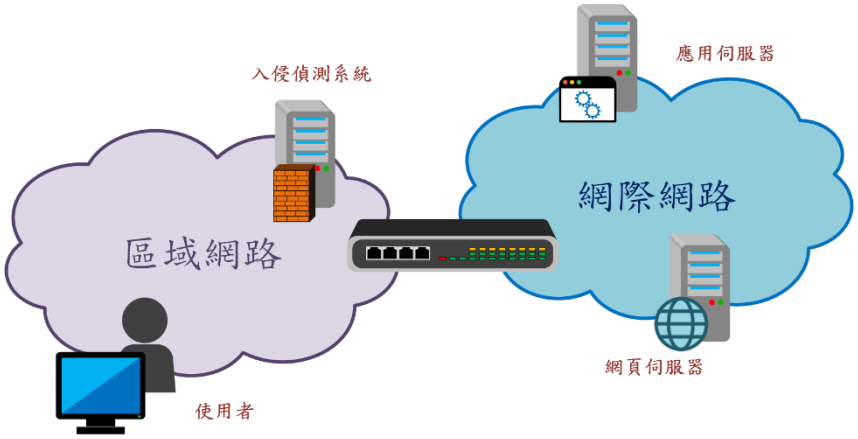
* 通訊作者 (Corresponding author.)

metaheuristic algorithm). The experimental results show that the proposed hybrid algorithm provides a better accuracy rate in solving complex network attack classification problems.

Keywords: Intrusion detection system, classification algorithm, and metaheuristic algorithm.

壹、前言

近年來有許多新型的網路攻擊方法，經由各式的途徑在網際網路中進行散佈。資料加密、防火牆、防毒軟體及入侵偵測等技術，可被視為目前網路安全防禦的代表性技術[1]。其中資料加密技術的主要概念是通過加密資料，防止惡意使用者竊取或竄改資料。而防火牆則利用硬體設備或安裝軟體設定安全通道，避免資料在網際網路間傳遞，被有心人士所竊取。舉例而言，防火牆可將網際網路區隔成信任區域與非信任區域，透過設置黑名單與白名單，讓特定使用者存取信任區域內之裝置，藉由限制特定資料與封包通過防火牆，達到保護區域內裝置與資料之安全。有別於其他對抗網路攻擊行為的方式，安裝防毒軟體可用來避免惡意使用者透過電腦病毒的方式，來攻擊特定電腦或特定網路區段。在這些技術中，入侵偵測系統 (intrusion detection system; IDS) 以類似於防火牆及防毒軟體的方式，來阻絕不當的攻擊行為。其主要的方式是透過分析流經所欲監控網路區域的網路封包、流量或網路行為，以事先建置的分類器，將不當網路行為進行阻絕。為了更進一步的提升網管系統的成效，蜜網 (honeynet) [2] 及入侵偵測防禦系統 (intrusion prevention system; IPS) [3]，這些與入侵偵測系統相關的技術，也在近年被使用於網路管理系統之中。如圖一所示，傳統的入偵測系統在使用者與外部應用伺服器建立連線時，封包由外部網際網路流入至內部區域網路時，我們可以將其複製一份，轉送至入侵偵測系統進行分析，透過分析結果可阻擋可疑的封包來源。但近年的資訊系統，通常會將所傳遞的封包內容進行加密，傳統的入侵偵測方式較難透過分析封包的內容來進行入侵偵測。



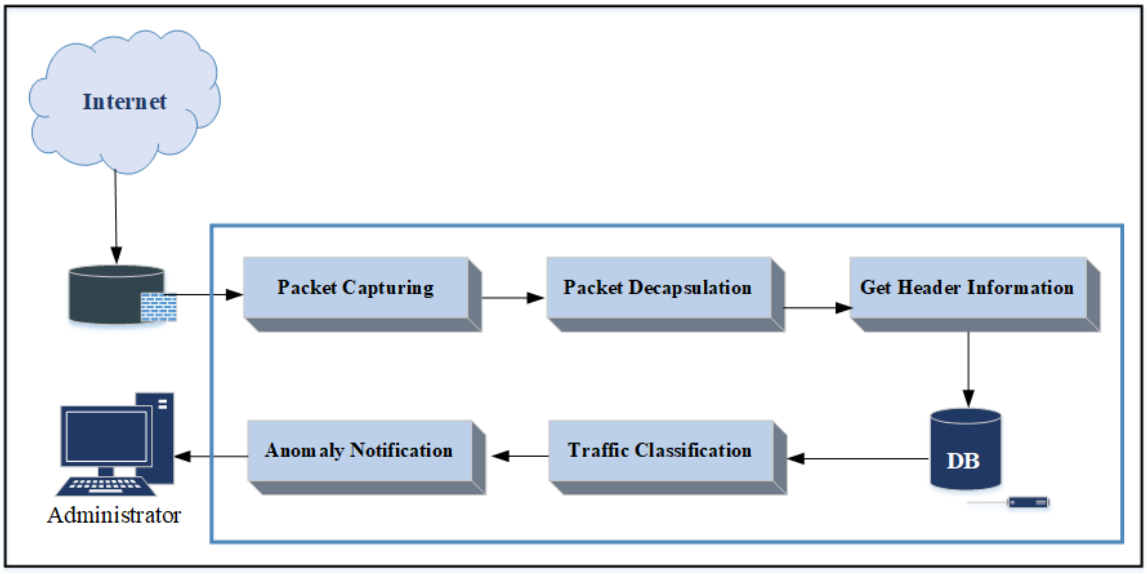
圖一、入侵偵測系統架構圖

從入侵偵測系統架設位置，入侵偵測系統可分成兩種類型 [4-5]:主機式入侵偵測系統 (host-based intrusion detection system; HIDS) 與網路端入侵偵測系統 (network-based intrusion detection system; NIDS)。主機式入侵偵測系統一般會安裝於系統中，透過偵測與分析紀錄檔，檢查是否有異常行為發生。網路端入侵偵測系統一般會建置於網路管理系統中，透過擷取封包、分析封包及制定規則，檢測網路異常使用行為，進一步使用更新分類規則技術，能夠達成快速辨識新型態之網路攻擊。根據入侵偵測的判斷方式，常見的入侵偵測可被分為: 誤用偵測 (misuse detection) 及異常偵測 (anomaly detection) [6-7]。其中誤用偵測的方式，主要是將所擷取封包與已知的攻擊型態資料進行比對，以偵測不當網路使用行為。異常偵測的方式，主要透過比較正常網路使用模式與當下網路使用模式之差異，判斷當前網路使用模式是否屬於異常。若使用者行為與正常行為差異過大，則會被判斷成攻擊行為。由於現今網路攻擊模式的快速發展，導致入侵偵測系統更新辨識方式之速度會比新型網路攻擊的產生較慢，如何在較短時間內更新系統判別模組，以辨識新型網路攻擊模式，因此成為此研究領域的一個重要研究課題。

為了提升入侵偵測系統的效能，本研究將以我們先前所提出的混合式策略 [8] 為基礎，來建置入侵偵測系統，稱之為 SEIDS (search economics-based intrusion detection system)。這個方法將藉由結合搜尋經濟學 (search economics; SE) 與 k 平均演算法 (k-means) 及支持向量機 (support vector machine; SVM)，可以降低系統的訓練時間與資料複雜度，進一步提升入侵偵測系統之準確率。本文的章節組織如下述描述。首先將於第貳章介紹現行入侵偵測系統的應用以及目前此類研究所需解決之問題。第參章將說明本研究所提出之混合式分類演算法，如何應用於入侵偵測系統之上。第肆章將說明本研究實驗環境、測試資料集，並藉由實驗結果來說明本研究所提出之方法效能。最後在第伍章將說明本研究之結論，以及未來可行研究方向。

貳、文獻探討

如圖二所示，早期的入侵偵測系統是基於深度封包檢測 (deep packet inspection; DPI) 的方式，將實體網路介面卡啟用混雜模式 (promiscuous mode) 功能，擷取流經網路介面卡之網路封包，透過分析封包內容來了解目前網路行為模式。但由於現行大部分的網路封包在傳送前會將其資料進行加密，這種傳統深度封包檢測方法，在現今網路環境較不適用。



圖二、深度封包檢測架構圖

近年許多研究嘗試改良現有入侵檢測系統，來提升其辨識不當網路行為之準確性。在研究 [9-10] 中，資料探勘及智慧型演算法被應用至入侵偵測系統，以提高此類系統對於不當網路行為判別之準確率。這些方法包含: *k* 個最近鄰居法 (*k* nearest neighbor; *k*-NN)、支持向量機 (support vector machine; SVM)、超啟發式演算法 (metaheuristic algorithm; MA) 和類神經網路 (artificial neural network; ANN) 等。在研究 [11] 中，Stein 等人進一步將決策樹 (decision tree) 與遺傳基因演算法 (genetic algorithm; GA) 進行整合，以一個混合式的方式來改良分類演算法的資料特徵選擇程序。其實驗結果說明這樣的混合策略，可以提升入侵偵測系統於網路異常檢測之準確率。Lin 等人在後續研究 [12] 中，進一步使用混合式超啟發式演算法 (hybrid metaheuristic algorithm)，來改良入侵偵測系統。這項方法將粒子群最佳化演算法 (particle swarm optimization; PSO) 與支持向量機進行整合，從訓練資料中選取較好的特徵集合降低資料維度。其所發展之入侵偵測系統，可以有效的減少計算時間與提升其準確率。由於智慧型方法在許多研究領域在近期已有許多成功的應用，Kuang 等人在近期的研究 [13] 中，嘗試以超啟發式演算法中的遺傳基因演算法，結合資料探勘方法中的支持向量機，訓練入侵偵測系統中之分類器。

其實驗結果說明這類的整合機制，有助於提升入侵偵測系統的準確度。

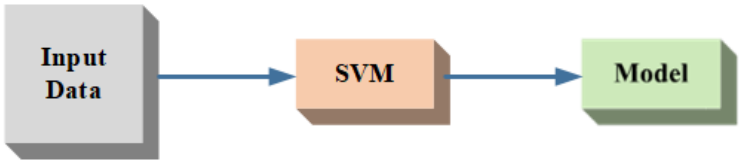
由於近年網路環境的攻擊模式變化相當快速，以傳統方式所建置的入侵偵測系統的分類器，無法辨識未知的網路攻擊。如何使入侵偵測系統有能力辨識未知的網路攻擊，近年逐漸成為的一項重要的研究趨勢。舉例而言，Tsai 在其研究 [14] 中將粒子群最佳化演算法結合 *k* 平均演算法，發展一個漸進式 (incremental) 的分類演算法，使這個分類演算法具有非監督式學習 (unsupervised learning) 及監督式學習 (supervised learning) 的特色，來使入侵偵測系統有能力可以偵測系統未知的攻擊。Saied 等人在後續的研究 [15] 中，更進一步的以類神經網路的方式來訓練分類器，來使系統有能力辨識未知的阻斷服務攻擊 (denial-of-service attack)。

在入侵偵測系統的相關研究中，目前仍有許多開放性的研究議題需被解決，這些議題包含: 訓練資料及的分佈不平均、訓練資料過於複雜、未知攻擊等。在訓練資料集分佈不平均的情況下，常見的方法是調整各個類別的訓練資料數量，以避免分類演算法在訓練過程，過度偏向特定類別，造成系統容易產生誤判。在資料集過於複雜的情況下 (例如:高維度或大筆數的資料集)，訓練分類器過程通常需要大量的記憶體及儲存空間，並且需要大量的計算時間，將會使入侵偵測系統無法在短時間內建立合宜的分類器，因此無法即時判別新型的攻擊。常見的方式是刪除冗餘資料與降低資料維度。在研究 [16] 中，Kashef 與 Nezamabadi-pour 嘗試採用蟻行最佳化演算法 (ant colony optimization)，從原始資料中挑選具有鑑別力的特徵進入訓練程序，可有效的降低訓練資料複雜度，並減少訓練分類器的時間。除了 [14-15] 的研究嘗試使入侵偵測系統有能力辨識未知攻擊，近期的研究 [17-18] 說明結合非監督式學習 (unsupervised learning) 的方式，來設計分類演算法判別未知攻擊，是目前的一個研究趨勢。

參、以搜尋經濟學為基礎之入侵偵測系統

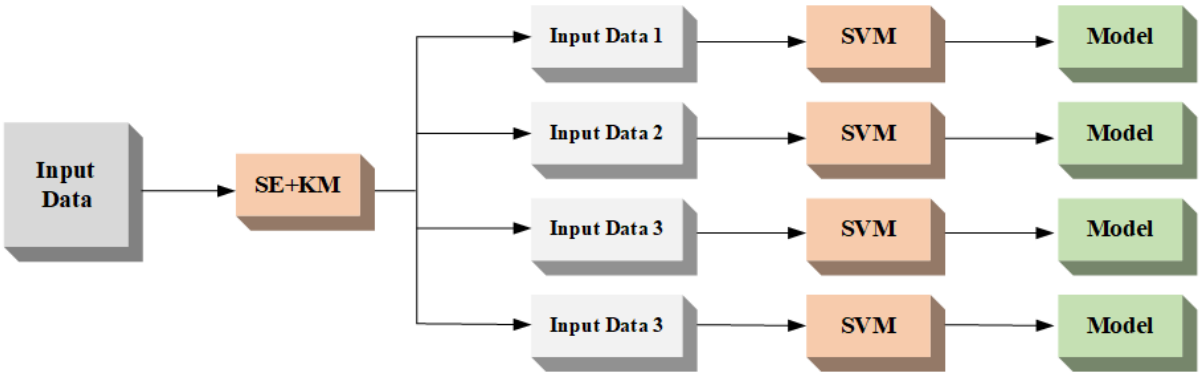
3.1 系統架構

本研究所提出系統，可分成兩個部分，分別為 SEKM (search economics + *k*-means) 以及 SVM，稱之為 search economics-based IDS (SEIDS)。基本的設計概念是將入侵偵測系統之監督式分類演算法，加上無監督式學習演算法，來提升入侵偵測系統辨識異常網路行為或網路攻擊之能力。SEKM 演算法的設計，是以我們先前所發展的一個新型超啟發式演算法 (search economics; SE) [19] 為基礎，結合 *k*-means 演算法，所發展出的一種高效能分群演算法。相較於傳統以支持向量機為基礎所設計的入侵偵測系統 (如圖三所示)，我們所發展的入侵偵測系統 (如圖四所示)，加入 SEKM 程序，將會以分群演算法在訓練資料進入分類器前，找出相似資料將其進行歸類，降低資料複雜度並且降低資料大小，節省分類演算法計算時間。

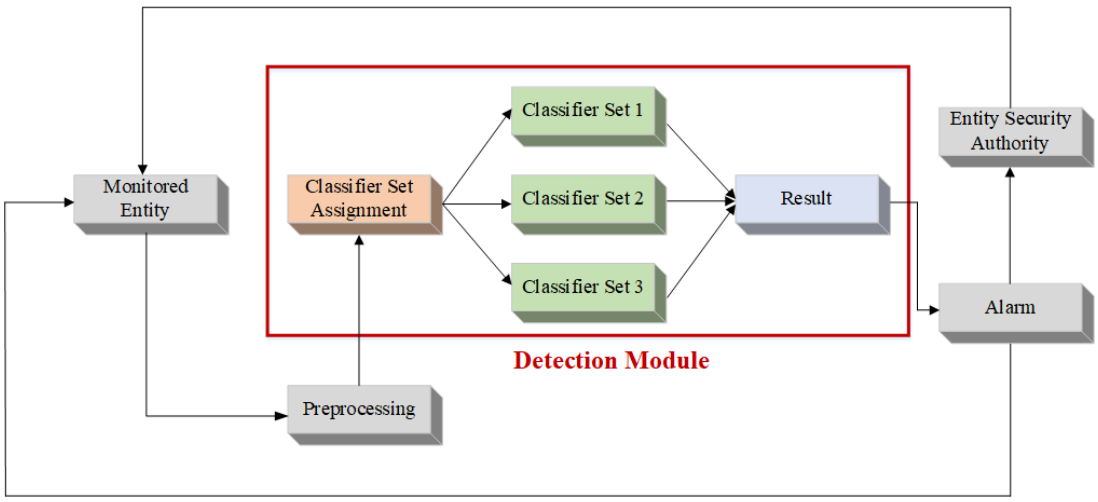


圖三、傳統支持向量機分類模型訓練過程

SEKM 演算法首先使用 *k*-means 分群演算法將輸入進行資料分群，透過 SE 演算法尋找最佳資料分群結果。這些分群結果將用於分割輸入資料 (如圖四 input data)，使其成為多個子資料集 (如圖四 input data 1)。而此入侵偵測系統將會分別將這些子資料集，放入不同的支持向量機進行模型訓練，產生多個分類模型。由於各子資料集相較於原始輸入資料集較小，訓練分類器過程將可以有效地縮短。相較於傳統的入侵偵測系統需要以集中式方式進行運算，這個設計方式更適合目前物聯網等分散式的網路環境。



圖四、SEKM + SVM 分類器訓練過程



圖五、本研究所發展之入侵偵測系統架構 (SEIDS)

如圖五所示，SEKM 結合 SVM 所訓練出的分類器，可被整合至入侵偵測系統，用以提升此系統效率。在入侵偵測系統擷取網路封包或使用者網路行為後，經由前處理程序將所蒐集的資料進行整理，傳遞至偵測模組 (detection module)，藉由資料分類方式，此系統會將所擷取的資料根據相似度計算，分配至與輸入資料較相似之分類器，進行網路行為辨識。相較於傳統的入侵偵測系統，這樣的設計方式，可以有效減少分類器訓練的計算時間，同時也能減少每次辨識過程中所需要的分類器，進而減少資料辨識的計算時間。

3.2 搜尋經濟學演算法架構

由於搜尋經濟學 (search economics; SE) 是一個新型的超啟發式演算法，在本研究中對於此演算法進行部分的改進，下面討論將介紹經濟搜尋演算法的基本架構和運作流程。圖六說明這個演算法基本計算程序。

Algorithm 1: Search Economics

```
Initialization()
ResourceArrangement()
While the termination criterion is not met do
    VisionSearch()
    MarketingReserch()
End While
Output Result
```

圖六、搜尋經濟學演算法

如圖六所示，SE 除了 Initialization()程序，ResourceArrangement()、VisionSearch()、及 MarketingReserch()為主要的三項程序。這個演算法的設計主要概念是將搜尋空間 (search space) 進行切割成數個子空間，以各子空間可能找到較佳解之期望值來取代傳統超啟發式演算法所使用的目標值 (objective value)，衡量是否要朝特定子空間前進，進一步搜尋可行解。其中 ResourceArrangement() 所負責的工作是將解空間切成多個子空間，並隨機產生 n 個候選解。VisionSearch()所負責的工作與一般的超啟發式演算法相同，將對現有的候選解進行解的轉換 (transition)、解的衡量 (evaluation) 以及決定 (determination) 後續搜尋方向 [20]。在這個研究中，我們使用突變 (mutation) 和 k-means 作為轉換解的方式。首先將隨機在候選解上進行突變，改變解的結構，再以 k-means 進行分群，若新產生的解比現行解較好，則由新產生的解取代現行解。在決定的程序中，這個演算法將使用期望值來對於各子空間進行評估，決定在特定的子空間增加投入或減少搜尋資源。期望值所考慮的資訊包含各子空間所新產生解的目標值、在各

子空間所投入的資源多寡以及目前各子空間所能找尋到最佳目標值，其詳細的計算方式可參考研究 [19]。MarketingResearch () 程序在這個演算法所扮演的角色是紀錄各子空間目前為止所能找到最好的可行解以及 SE 在每個子空間所搜尋的次數。在每一迭代 (iteration) 之後，更新每個子空間內的相關資訊，使整體的搜尋可以依據各子空間所投資的資源多寡以及各子空間所能找到的最佳可行解，來決定往哪個子空間進一步的搜尋。透過這個方式，SE 可以避免朝向特定區域或方向前進，因此可以避免搜尋過程過快的掉入區域最佳解。相較於傳統的超啟發式演算法，SE 可以有效地在搜尋過程中，維持搜尋的多樣性 (search diversity)，並依據各子空間的潛力來動態調整搜尋資源，因此能夠在一些最佳化問題中，找到比傳統超啟發式演算法更好的結果。

肆、實驗結果

4.1 資料集

本研究實驗使用 Power System Datasets、NSL-KDD、CIDDS-001、GPRS-WPA2 及自訂的資料集，進行實驗模擬。其中 Power System 資料集 [21] 的內容是智慧電網之電力使用資料，因原始資料集較多，本實驗將使用這項資料中的三個資料集進行實驗，用來測試不同的入侵偵測分類演算法，於工控環境下對於不當網路行為之辨識效能。另一個資料集 [22] 是 KDD99，經由刪除多筆冗餘資料，可被用來測試入侵偵測系統的效能，稱為 NSL-KDD。雖然這個資料集已經不能代表現代網路複雜程度，但仍有許多研究繼續使用該資料集測試效能，可被視為測試入侵偵測分類演算法效能的一個基礎資料集。CIDDS [23] 和 GPRS [24] 是兩個新型的測試資料集，CIDDS 是模擬小型企業環境，紀錄正常網路流量和常見的網路攻擊模式，而 CIDDS 資料集屬於連續紀錄且紀錄時間較長，資料集較為龐大，本研究中的實驗只使用其部分資料。GPRS 資料集是一個記錄無線網路的環境，這個資料集具有兩種不同的拓撲結構 (WEP/WPA 及 WPA2)。最後一個資料集屬於混合資料集，來自於多個真實網路的封包 [25-28] 混合而成。表一說明這些資料集詳細資訊，其中包含各資料集之資料筆數、資料容量大小、類別數量、特徵數量。

表一:實驗用資料集詳細資訊

Dataset		Training		Testing		Classes	Attributes
		Instances	Size	Instances	Size		
DS1	Power System	3,974	4.2MB	993	1.1MB	3	128
DS2	Power System	3,974	4.2MB	993	1.1MB	3	128
DS3	Power System	3,974	4.2MB	993	1.1MB	3	128
DS4	NSL-KDD	125,973	19.1MB	22,544	3.4MB	5	41
DS5	CIDDS-001	7,999	441.7KB	17,669	984.7KB	5	11
DS6	GPRS-WPA2	7,500	330.4KB	2,500	110.3KB	5	16
DS7	Synthetic	125,973	19.1MB	18,663	1.8MB	5	16

4.2 衡量方法

本研究中我們將使用四個衡量指標，針對所提出之方法進行衡量，分別為檢測 (recall)、誤報率 (false alarm rate, FAR)、精密度 (precision) 和準確率 (accuracy)。這四項衡量指標定義如下:

$$\text{DR} = \frac{TP}{TP + FN} \tag{1}$$

$$\text{FAR} = \frac{FP}{TN + FP} \tag{2}$$

$$\text{Precision} = \frac{TP}{TP + FP} \tag{3}$$

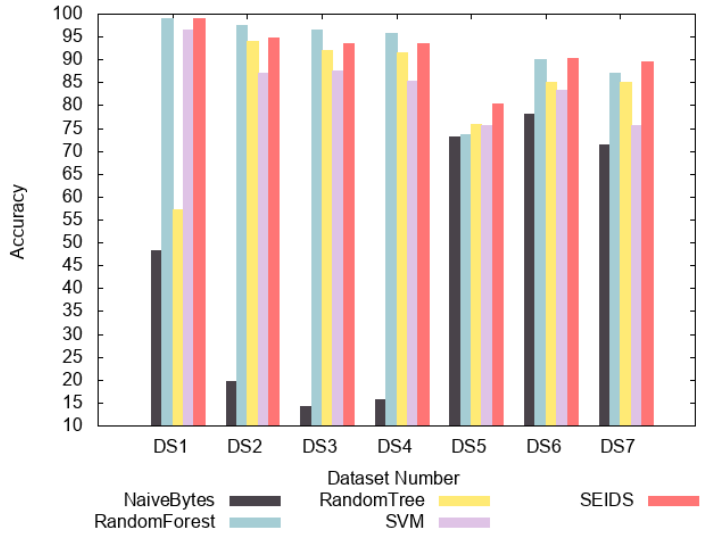
$$\text{AR} = \frac{TP + TN}{TP + FP + TN + FN} \tag{4}$$

其中 TP 為 true positive，TN 為 true negative，FP 為 false positive，FN 為 false negative。DR、Precision與AR數值越高，代表其系統的辨識準確率越好，而FAR為錯誤檢測的機率，出現越低的數值代表其系統將正常網路行為判別為異常的機率越低。

4.3 實驗結果 1-多類別辨識

此實驗的設計是讓入侵偵測系統將所有網路資料分類成數個類別，分類演算法必須擁有識別攻擊類型的能力，每筆資料都需要被歸類到正確的類別之中。圖七為本研究提出之系統 (SEIDS) 和其他分類演算法的比較。其結果顯示 SEIDS 在工控資料集 (DS1 至 DS3) 中，雖然無法取得最佳成果，但準確率都能維持在 95%左右，其原因為工控網路環境資料集相較於一般網路環境簡單，所以許多演算法都能有不錯的效能。另一方面在 DS5 至 DS7，SEIDS 都能達到最好的效果，因此說明在面臨複雜的網路資料時，SEIDS

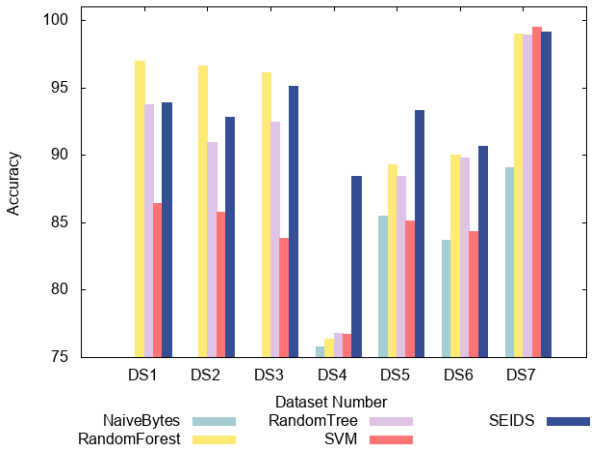
對於不當的網路行為，可以有較好的辨識能力。在另一方面，SEIDS 所採用分類演算法為 SVM，由於本研究提出演算法可先降低資料的複雜度，結果顯示這個方法能在大多數的資料集中，比單獨使用 SVM 的結果更準確。這些結果更顯示 SEIDS 在 CIDSS 和 GPRS 這兩個資料集，可達到最好的檢測效果，說明此方法可能更適合現代的網路架構。



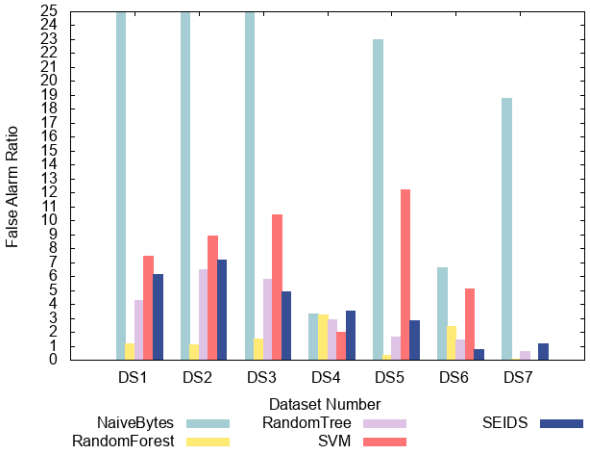
圖七、多分類問題實驗結果

4.4 實驗結果 2-二類別辨識

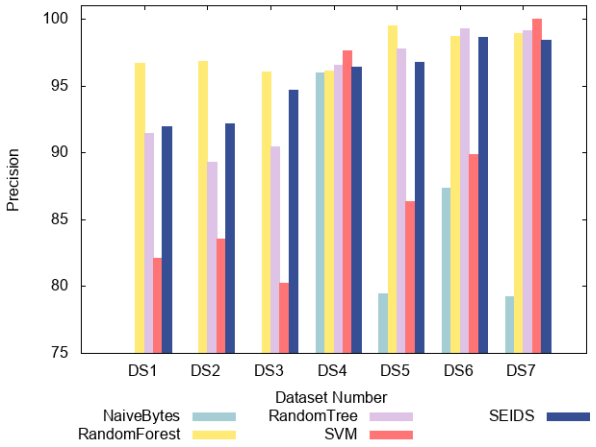
這個部份的實驗是將檢測資料集，轉換成正常與攻擊的二分類問題。如圖八所示，實驗結果顯示前三個資料集中，SEIDS 都能取得不錯的效果。雖然在工控資料集中，SEIDS 如實驗結果 1 一樣無法取得最佳的辨識率，但仍有 90%以上的準確率，其誤報率也處於一個合理的範圍。相較於一般的 SVM 的衡量結果，因 SEIDS 可降低資料集複雜度，可讓 SVM 的分類效果有顯著提升，使其能夠在 DS4-DS7 四個資料集，達到不錯的結果。在 DS4 的測試結果中，可發現其他分類演算法之準確率都低於 80%以下，但 SEIDS 之準確率卻能達到 88.45%之準確率，說明 SEIDS 在將網路行為改為二分類問題時，其具備一個較穩定的檢測效果。



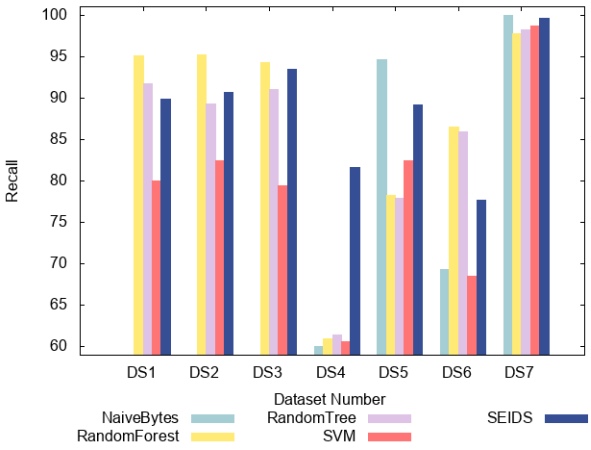
(a) 準確率 (accuracy)



(b) 誤報率 (FAR)



(c) 精密度 (precision)



(d) 檢測率 (recall)

圖八、二分類問題實驗結果

伍、結論

本研究提出了一種全新的混合式入侵偵測分類演算法，該分類演算法的概念是改良自於超啟發式演算法中的搜尋經濟學演算法，並結合分群演算法的 *k*-means 演算法及分類演算法的支持向量機。由於本研究中所提出的混合式演算法比其他方法在收斂過程中擁有搜尋多樣性，從實驗結果中可觀察出混合式分類演算法可提升入侵偵測系統檢測準確率。未來研究將分成兩部份，其一是開發出更有效率、更高的準確率以及降低誤報率的方法，另一部分則是將本研究提出之方法應用於各式網路環境，例如雲端計算平台或物聯網環境。

致謝

本研究由科計部計畫 MOST 107-2221-E-110 -078 及 MOST 107-2218-E-005 -018 補助支持，特此誌謝。

參考文獻

[1] W. Stallings and L. Brown, Incident Response: *Computer Security Principles and Practice*, Prentice Hall Press, 2014.

[2] A. Mairh, D. Barik, K. Verma and D. Jena, "Honeypot in network security: A survey," in *Proceedings of the International Conference on Communication, Computing & Security*, pp. 600-605, 2011.

[3] A. Patel, M. Taghavi, K. Bakhtiyari and J. C. Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 25-41, 2013.

[4] H. J. Liao, C. H. R. Lin, Y. C. Lin and K. Y. Tung, "Intrusion detection system: A comprehensive review," *Network and Computer Applications*, vol. 36, no. 1, pp. 16-24, 2013.

[5] T. F. Lunt, "A survey of intrusion detection techniques," *Computers & Security*, vol. 12, no. 4, pp. 405-418, 1993.

[6] I. Burguera, U. Zurutuza and S. Nadjm-Tehrani, "Crowdroid: Behavior-based malware detection system for android," in *Proceedings of the ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pp. 15-26, 2011.

[7] C. Michel and L. Mé, "ADeLe: An Attack Description Language for Knowledge-Based Intrusion Detection," *in Proceedings of the IFIP International Information Security Conference*, pp. 353-368, 2001.

[8] Z.H. Chen and C.W. Tsai, "An Effective Metaheuristic Algorithm for Intrusion Detection System," *in Proceedings of the IEEE International Conference on Smart Internet of Things*, pp. 154-159, 2018.

[9] K. C. Lee and L. Mikhailov, "Intelligent intrusion detection system," in *Proceedings of the International IEEE Conference on Intelligent Systems*, vol. 2, pp. 497-502, 2004.

[10] O. Depren, M. Topallar, E. Anarim, and M. K. Ciliz, "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks," *Expert Systems with Applications*, vol. 29, no. 4, pp. 713-722, 2005.

[11] G. Stein, B. Chen, A. S. Wu, and K. A. Hua, "Decision tree classifier for network

intrusion detection with GA-based feature selection," in *Proceedings of the Annual Southeast Regional Conference*, vol. *2*, pp. 136-141, 2005.

[12] S. W. Lin, K. C. Ying, S. C. Chen, and Z. J. Lee, "Particle swarm optimization for parameter determination and feature selection of support vector machines," *Expert Systems with Applications*, vol. 35, no. 4, pp. 1817-1824, 2008.

[13] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," *Applied Soft Computing*, vol. 18, pp. 178-184, 2014.

[14] C.W. Tsai, "Incremental Particle Swarm Optimization for Intrusion Detection," *IET Networks*, vol. 2, no.3, pp.124-130, 2013.

[15] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDOS attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385-393, 2016.

[16] S. Kashef and H. Nezamabadi-pour, "An advanced ACO algorithm for feature subset selection," *Neurocomputing*, vol. 147, pp. 271-279, 2015.

[17] R. A. R. Ashfaq, X. Z. Wang, J. Z. Huang, H. Abbas, and Y. L. He, "Fuzziness based semi-supervised learning approach for intrusion detection system," *Information Sciences*, vol. 378, pp. 484-497, 2017.

[18] P. Casas, J. Mazel, and P. Owezarski, "Unsupervised network intrusion detection systems: Detecting the unknown without knowledge," *Computer Communications*, vol. 35, pp. 772-783, 2012.

[19] C. W. Tsai, "An effective WSN deployment algorithm via search economics," *Computer Networks*, vol. 101, pp. 178-191, 2016.

[20] C. Blum and A. Roli, "Metaheuristics in combinatorial optimization: Overview and conceptual comparison," *ACM Computing Surveys*, vol. 35, no. 3, pp. 268-308, 2003.

[21] https://sites.google.com/a/uah.edu/tommy-morris-uah/ics-data-sets, Available: 2019/02/22.

[22] http://www.unb.ca/research/iscx/dataset/iscx-NSL-KDDdataset.html, Available: 2019/02/22.

[23] D. W. F. L. Vilela, E. W. T. Ferreira, A. A. Shinoda, N. V. de Souza Arajo, R. de Oliveira, and V. E. Nascimento, "A dataset for evaluating intrusion detection systems in IEEE 802.11 wireless networks," in *Proceedings of the IEEE Colombian Conference on Communications and Computing*, pp. 1-5, 2014.

[24] M. Ring, S. Wunderlich, D. Grdl, D. Landes, and A. Hotho, "Flow-based benchmark data sets for intrusion detection," in *Proceedings of the 16th European Conference on Cyber Warfare and Security*, pp. 361-369, 2017.

[25] https://github.com/VishwaPrabhakar/MaliciousIPScanner/blob/master/goldeneye.pcap, Available: 2019/02/22, Available: 2019/02/22.

[26] https://github.com/somethingnew2-0/CS642-HW2/blob/master/traces/synflood.pcap, Available: 2019/02/22, Available: 2019/02/22.
[27] https://github.com/onty/trace-samples/blob/master/DIAMETER/ESy/EsyAndGy-Normal.pcap, Available: 2019/02/22, Available: 2019/02/22.
[28] https://www.dropbox.com/sh/kk24ewnqi9qjdvt/AAAz0ySsffUi8B8yoPSE5kc3a/pcaps?dl=0, Available: 2019/02/22.