整合分類演算法提升網路入侵偵測系統效能之研究

作者／曾鴻麟少校

提要

一、入侵偵測系統(Intrusion Detection System, IDS)因各式各樣的網路行為及頻繁的進出流量，產生龐大的資料。而國軍在歷經組織調整轉型的過程中，員額逐次精簡，各部隊資訊管理人力普遍不足，以人力篩選或建立入侵偵測系統規則將造成莫大的負擔，若能運用資料探勘技術則可協助規則的建立。

二、集成系統又稱為整體學習(Ensemble Learning)，若能運用集成系統之整合策略，結合多種不同特性之分類器，來推論出最後分類結果，便可避免單一分類器之分類錯誤。

三、本研究提出強化式整合學習(Enhanced Integrated Learning, EIL)演算法與基於EIL 演算法集成系統(EIL-Algorithm Based Ensemble System, EILBES)來解決少數攻擊類別偵測率不佳的問題，經由實驗證實可成功改善網路異常入侵偵測分類效能。

關鍵詞：入侵偵測、資料探勘、集成系統。

前言

近年來資訊科技幾乎已成為生活中不可或缺的一部分，經過數位化後，昔日一整間圖書館的書，在一個拇指大的隨身碟內就可存放。數個櫃子的 CD，能存在隨身手機或撥放器中，讓我們隨時聆聽，就連世界各地發生的事，都能立即在網際網路上看到，這些科技雖然帶來了便利，但是利用這些科技進行的攻擊事件也越來越頻繁。因此，為了防護網路攻擊，在一個完整的縱深防禦架構中，入侵偵測系統就成為重要的一道防線，用來協助抵抗外部的攻擊。入侵偵測系統主要藉由監控網路活動，收集網路上的封包，或是配合防火牆與其他資安系統所取得的資訊，根據本身資料庫進行比對，判斷為正常流量或是異常行為，做出即時的處理，然而如何提高入侵偵測系統的效能，一直是資訊安全系統重要的研究方向。

各式各樣的網路行為及頻繁的進出流量，使入侵偵測系統產生龐大的資料，以人力篩選或建立入侵偵測系統規則將造成莫大的負擔。而國軍在歷經組

織調整轉型的過程中，員額逐次精簡，各部隊資訊管理人力普遍不足，若能運用資料探勘技術則可協助規則的建立。但是，至今運用資料探勘技術在入侵偵測系統的偵測方法設計上，仍然有許多問題需要克服，如單一分類器對少數重要入侵類別的預測，常會有偵測率不佳、準確率低等情況。因此，本研究目的是運用資料探勘技術，針對入侵偵測系統提出一套演算法機制，希望能夠整合知識發掘過程中各階段效能良好的改善機制，強化系統分類能力，提升入侵偵測系統整體效能，有效對抗網路攻擊事件。

相關文獻

一、入侵偵測系統介紹

入侵偵測系統的架構依照防護範圍主要可分為主機型入侵偵測系統(Host-Based IDS)及網路型入侵偵測系統(Network-Based IDS) 。[1]依入侵偵測系統偵測方式不同可分為誤用偵測型(Misuse Detection)及異常偵測型(Anomaly Detection)，[2]主要是利用收集到的資料來分析網路行為，當發現攻擊行為後，便採取警報、處理及紀錄等方式因應。

二、資料探勘技術介紹

資料探勘是資料庫知識發掘(Knowledge Discovery in Database, KDD)中的一個不可或缺的部分，可從大量資料庫中發掘出重要與潛藏資訊的過程。[3]

(一)集成系統

集成系統又稱為整體學習(Ensemble Learning)、多重分類器系統(Multiple Classifier Systems)、分類器委員會(Committee of Classifiers)或混合式專家系統(Mixture of Experts)等。在攻擊手法日新月異下，入侵偵測系統也因雜訊、不平衡的樣本分布等影響，面臨偵測效能不佳的問題。因此，若能運用集成系統整合策略，結合多種不同特性的分類器，來推論出最後分類結果，便可避免單一分類器的分類錯誤。就像看病時，醫生如告知得了某種重症，病人會再找其他名醫看診，以確定自己的病情。就算是儀器，也有機會出錯，如能結合不同儀器，不同醫師診斷意見，的確能降低單一的錯誤判斷機率。

學者Polikar指出：影響集成系統效果的重要因素，在於系統內分類模型。

---

[1]Doyle, J., Kohane, I., Long W., Shrobe, H., and Peter, S., "Event Recognition Beyond Signature and Anomaly," Proceedings of the 2001 IEEE, Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 2001, pp.17-23.

[2]同註 1，pp.17-23。

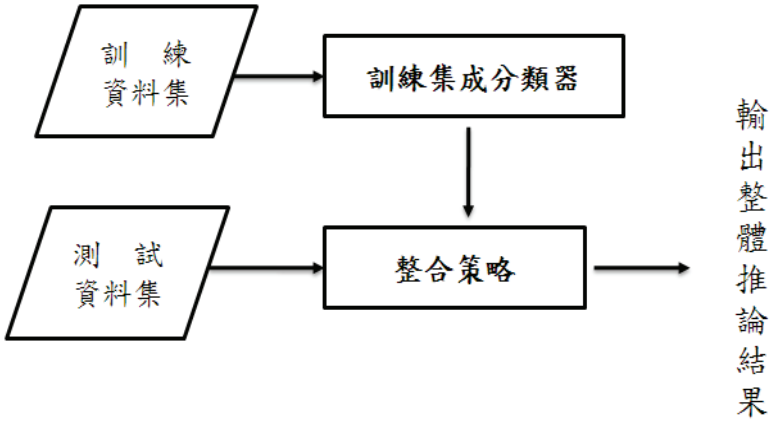
[3]Tan, P. N., Steinbach, M., and Kumar, V., Introduction to Data Mining, (U.S.A:MORGAN KAUFMANN PUBLISHERS, 2006, U.S.A, pp.4-9.

差異性(Diversity)應該要盡可能越大越好。[4]若系統內各分類模型差異性大，且有一定的準確率，則各分類模型所分類錯誤的樣本也就越不相同。因此，一個樣本同時被所有分類模型分類錯誤的機率將大幅降低，最後結合這些個別分類模型的輸出，得到最終推論結果之錯誤機率也大幅降低。也就是說，越有可能將原本錯誤分類的樣本正確地區分出來。

要提升集成系統內分類模型的差異性，主要有以下四種方法：使用不同的訓練資料集、對於各個分類模型採用不同的參數設定、使用不同的演算法、使用不同的特徵等方法來訓練不同的分類模型。[5]

集成系統的架構圖（如圖一）包含兩個重要的步驟。首先第一步驟為建立集成系統的分類器，就是先訓練出集成系統中各個獨立且具差異性的分類模型；第二步驟則是整合策略，用來結合集成系統內不同分類模型輸出的推論結果[6]。在現實的情況中，因受到雜訊、不平衡的樣本分布等影響，很難訓練出具有泛化能力的分類模型，所以在運用單一分類模型無法獲得滿意的推論能力時，可運用集成系統來整合多個分類模型的推論能力，並從中得到整體最佳的分類效果。

圖一 集成系統架構圖



資料來源：詹益東，〈網路異常入侵偵測分類效能改善方法〉(桃園：國防大學中正理工學院資訊科學所碩士論文，2010 年)，頁 35。

(二)分類技術的評估方式

分類效能的評估，在於利用測試資料集被分類模型正確分類與錯誤分類的數量來決定，一般來說會建立可用來計算準確率(Accuracy)與錯誤率(Error

[4]Robi Polikar, “Ensemble based systems in decision making,” IEEE Circuits and Systems Magazine, Vol.6, 2006, pp. 21-45.
[5]同註 4，pp. 21-45。
[6]同註 4，pp. 21-45。

Rate)等衡量指標的混亂矩陣(Confusion Matrix)，[7]相關內容請參閱參考文獻七。

(三)特徵選取

在分類任務中，可能會面臨到有很多特徵的情況，而其中有一些特徵卻可能是不相關或是多餘的。一般情況下，入侵偵測系統需要處理大量的資料，會消耗相當多的資源，若資料中包含不相關或冗餘的特徵，將在訓練及測試的過程中，損耗更多的資源，造成較長的訓練時間及較差的偵測效能，所以刪除這些無關或冗餘特徵是非常重要的。

為了解決上述問題並建立更為準確的分類模型，運用特徵選取是一種有效的方式。特徵選取是資料探勘中極重要的技術，目標是希望能在全部的特徵中，挑選出對預測有幫助的最佳特徵子集，經研究證實，透過選擇重要和有效的特徵，可降低資料維度，不但能減少計算成本，更有助於提升資料探勘的效能。[8]

雖然特徵選取有助於提升資料探勘的效能，但是若忽略不平衡資料集的影響，會使分類效能不佳的少數類別，情況更是雪上加霜。欲提升少數類別準確率，就必須選擇對少數類別有較大影響的重要屬性，文獻[9]透過演算法平衡資料集後，配合ReliefF演算法找出重要特徵，經實驗證實能有效提升少數類別分類效能。

三、重要演算法介紹

(一)決策樹演算法

本研究所使用之分類技術以監督式學習為主，而決策樹演算法是其中最常被使用的分類學習演算法，相關內容請參閱參考文獻七。

(二)可適式回饋機制演算法

可適式回饋機制演算法(Adaptive Feedback Mechanism Algorithm, AFMA)[10]，用來強化特定少數類別的偵測率，並已證實可提升入侵偵測系統的效能，相關內容請參閱參考文獻七。

(三)中位數平衡化取樣機制演算法

文獻[11]提出中位數平衡化取樣機制演算法(Balanced Median-based Sampling Mechanism Algorithm, BMSMA)，結合綜合式仿製演算法(Synthetic

[7]潘致誠，〈強健式網路入侵偵測演算法則之研究〉(桃園：國防大學中正理工學院資訊科學所碩士論文，2009 年)，頁 18。
[8]Abu H. M Kamal, Xingquan Zhu, Abhijit Pandya and Sam Hsu, “Feature Selection with Biased Sample Distributions,” IEEE IRI 2009, 2009, pp.23-27 .
[9]同註 7，頁 49。
[10]同註 8，頁 26。
[11]同註 7，頁 41。

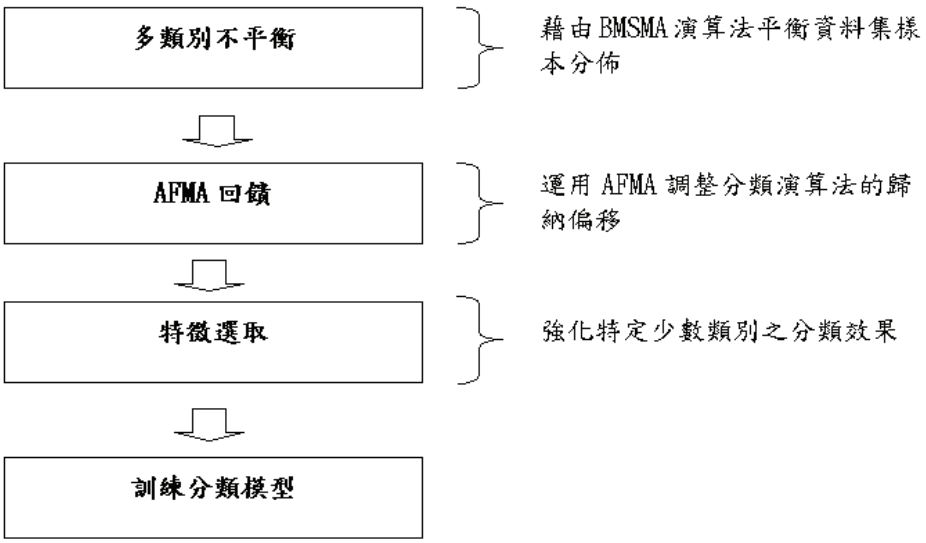
Minority Over-Sampling Technique, SMOTE)[12]方法來解決不平衡資料集的問題，以及改善標準中位數取樣法(Standard Median, SMedian)[13]容易過度學習之問題，並經實驗證明確實改善了不平衡資料集分類效能。

演算法首先尋找資料集中的中位數，接下來則檢查資料集中每一個類別的樣本數量。若樣本數量大於中位數，則利用隨機降低取樣方法，將該類別族群之數量取樣到和中位數一樣。若樣本數量小於中位數，則利用SMOTE演算法來創造新的類別樣本，直到類別的樣本數量和中位數一樣為止。如此一來，資料集中每一個類別的樣本數量將相同(等於中位數)，最後可輸出平衡化之訓練資料集。[14]

(四)整合式不平衡學習演算法

文獻[15]針對少數類別偵測效能不佳的情形，並考量不平衡資料集問題、特徵選取的重要性及可適式回饋機制演算法的強化性，提出整合式不平衡學習演算法(Integrated Imbalanced Learning Algorithm, IILA)，有助於少數攻擊類別偵測率的提升，演算法流程如圖二。

圖二 整合式不平衡學習演算法之流程圖



資料來源：詹益東，〈網路異常入侵偵測分類效能改善方法〉(桃園：國防大學中正理工學院資訊科學所碩士論文，2010 年)，頁 42。

IILA的目的在結合BMSMA對不平衡資料集的平衡化策略、AFMA對特定

[12]N.V. Chawla, K.W. Bowyer, L.O. Hall, and W.P. Kegelmeyer, "SMOTE:Synthetic Minority Over-Sampling Technique," Artificial Intelligence Research, Vol.16, 2002, pp.321-357.
[13]Naeem Seliya, Zhiwei Xu, and Taghi M. Khoshgoftaar, "Addressing Class Imbalance in Non-Binary Classification Problems," 20th IEEE International Conference on Tools with Artificial Intelligence, 2008, pp.460-465.
[14]同註 7，頁 41。
[15]同註 7，頁 38。

少數類別偵測率之強化和ReliefF演算法之特徵選取方法，達到互補與強化的最佳整體分類效果，以改善現今資料探勘型入侵偵測系統技術的缺點，經由實驗證實，IILA能有效強化分類模型，提升入侵偵測系統之效能。[16]

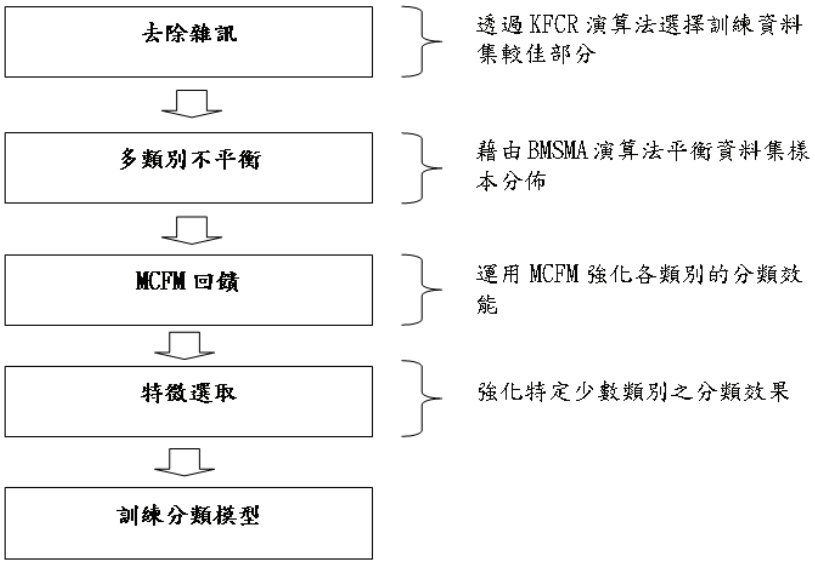
演算法設計

前述整合式不平衡學習演算法，成功結合多種不同演算法的優點，藉由可強化少數類別偵測率的特徵選取方式，解決不平衡資料集、多類別不平衡與歸納偏移等問題。若能增加對資料集的篩選，並將可適式回饋機制演算法只針對單一類別回饋的缺點改善，應該能發揮更好的分類效能。

一、強化式整合學習演算法

本研究以 k 倍交叉剔除(k-fold Cross Removing, KFCR)演算法，篩選訓練資料集中較佳的訓練樣本，並提出多類別回饋機制(Multi Classes Feedback Mechanism, MCFM)演算法改進 AFMA 只針對單一類別回饋的缺點。最後整合及改良 IILA，提出強化式整合學習演算法，演算法概念如圖三，各階段演算法分述如後。

圖三 強化式整合學習演算法之概念圖



資料來源：作者整理。

(一)k倍交叉剔除演算法

KFCR演算法運用取樣技術，達到篩選較佳訓練資料的目的，相關內容請參閱參考文獻七。

[16]同註 7，頁 50。

(二)多類別回饋機制演算法

重要演算法介紹中提到的可適式回饋機制演算法[17]，能用來強化特定少數類別的偵測率，但是觀察其演算法回饋機制，對目標類別之外的其他類別，並無強化功能，若能利用可適式回饋機制演算法的回饋機制，對所有類別進行強化，應該能提升整體的分類效能。故針對此點，本論文提出多類別回饋機制演算法，演算法步驟如表一。

強化式整合學習演算法透過KFCR演算法選擇訓練資料集較佳部分，藉以提升訓練資料集的訓練效能，接著藉由BMSMA演算法來平衡資料集樣本的分布，然後運用MCFM演算法來強化各類別的分類效能，最後將所得到的樣本經由ReliefF演算法進行特徵選取，以強化特定少數類別的分類效果。

表一 多類別回饋機制演算法步驟

步驟一	訓練模型：選定分類演算法，運用訓練資料集訓練模型。
步驟二	驗證模型：以驗證資料驗證訓練模型，並記錄各類別 Recall。
步驟三	決定回饋數量：以各類別被分類錯誤的資料數量中的最小值，定為各類別回饋數量。
步驟四	選擇回饋資料：將各類別被分類錯誤的資料，隨機降低取樣至回饋數量。
步驟五	回饋誤判資料：將步驟四各類別選出之分類錯誤資料回饋至訓練資料集，重複訓練新的訓練模型，以強化辨識率。
步驟六	判定訓練終止條件：重複步驟二至五，直到任一類別 Recall 到達 100%。

資料來源：作者整理。

二、基於EIL演算法集成系統

雖然本研究提出的 EIL 演算法能整合多種演算法，達到篩選較佳訓練資料、平衡資料集樣本分布及強化各類別分類效能的成效，但是單一分類器仍然無法避免單一錯誤推論的機率，若能利用集成系統的優點，結合多種不同特性之分類器，來推論出最後分類結果，便可避免單一分類器之分類錯誤，有效提升入侵偵測系統整體分類效能。因此本研究結合 EIL 演算法和集成系統的原理，提出基於 EIL 演算法集成系統(EIL-Algorithm Based Ensemble System, EILBES)來強化 EIL 演算法在重要類別 U2R 分類效能及整體準確率，更進一步提升入侵偵測系統整體效能。

資料探勘技術介紹中提到集成系統內分類器的差異性，若差異性越大，且

[17]同註 8，頁 26。

具有一定的準確率，則集成系統的效果越好，本研究利用 EIL 演算法訓練不同的獨立分類器，產生訓練樣本的差異性如下：

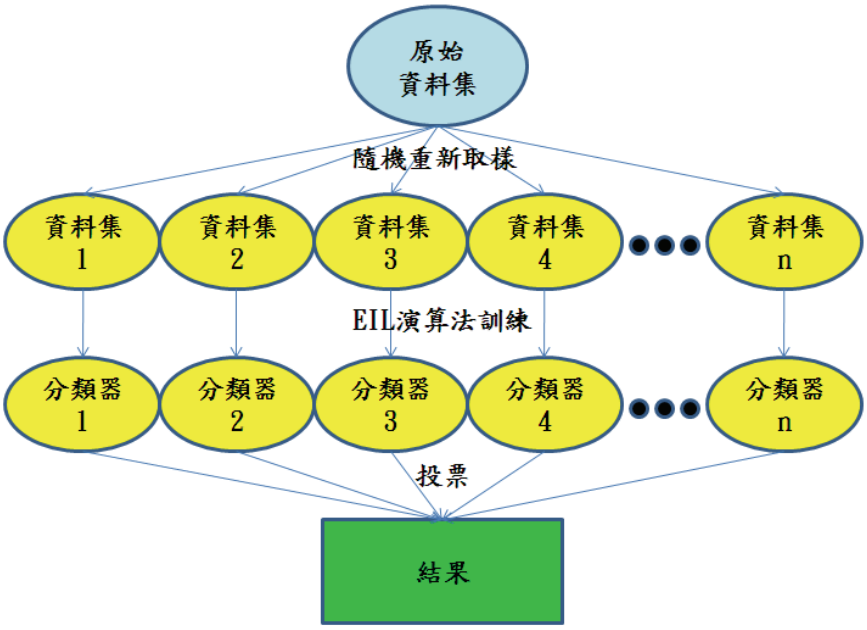
(一)資料前處理階段，KFCR演算法產生的訓練樣本差異。

(二)平衡資料集階段，BMSMA演算法產生的訓練樣本差異。

(三)錯誤回饋階段，MCFM演算法產生的訓練樣本差異。

演算法進行的步驟為當原始資料集輸入後，首先隨機取樣產生 n 個新資料集，接著運用 EIL 演算法得到 n 個分類器，最後使用多數投票制(Majority Voting)來結合 n 個分類模型的推論，根據所獲得最多票數之類別，做為 EILBES 之推論結果，演算法示意圖如圖四。

圖四 基於 EIL 演算法集成系統示意圖



資料來源：作者整理。

實驗設計與分析

本研究以 Weka 3.7[18]和 JAVA 程式語言來建構實驗環境，分類演算法選擇決策樹演算法，資料集採用 KDD99 入侵偵測資料集[19]。由於完整 KDD99 資料集的資料過於龐大，因此本實驗採用一般研究常用的 10%訓練資料集，亦即以 kddcup.data_10_percent 資料檔內容為訓練資料，再以 corrected 檔案內容為測試資料，實驗資料集數量及事件類別等相關內容請參閱參考文獻七。

實驗分為三部分：第一部分進行 AFMA 及 MCFM 演算法的比較；第二部分為 EIL 演算法的實驗；第三部分為基於 EIL 演算法集成系統的實驗。

[18]http://www.cs.waikato.ac.nz/ml/weka/, 2011/4/20.
[19]http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 2011/4/20.

一、KDD99資料集介紹

KDD99 資料集是最常被用來驗證入侵偵測系統效能的資料集，資料集的相關內容請參閱參考文獻七。

二、AFMA及MCFM演算法的比較

重要演算法介紹中提到的可適式回饋機制演算法，能用來強化特定少數類別之偵測率，但是對目標類別之外的其他類別，並無強化功能。第一部分實驗之目的在證實 MCFM 演算法可強化 AFMA 對其他類別的分類效能。

本實驗採用決策樹演算法作為分類演算法，訓練資料集為經過 KFCR 演算法的 KDD 99 10%訓練資料集，最後同樣以測試資料集驗證分類模型的效能，實驗結果如表二。

表二 AFMA 及 MCFM 演算法的比較結果

類別	演算法 評估指標	KFCR-DT	KFCR-AFMA	KFCR-MCFM
Normal	Recall	**99.48**	99.42	99.39
	Precision	73.52	73.10	**73.75**
	F-measure	84.55	84.26	**84.67**
DoS	Recall	97.21	97.2	**97.5**
	Precision	**99.88**	99.78	99.87
	F-measure	98.53	98.48	**98.67**
Probe	Recall	**80.84**	75.13	78.22
	Precision	79.19	**92.74**	79.44
	F-measure	80.01	**83.01**	78.83
U2R	Recall	10.53	12.71	**14.03**
	Precision	**80**	64.44	65.3
	F-measure	18.6	21.24	**23.1**
R2L	Recall	6.13	**7.59**	3.65
	Precision	**96.22**	95.64	71.72
	F-measure	11.52	**14.07**	6.94
	Accuracy	92.63	92.61	**92.66**

資料來源：作者整理。

在表二中，KFCR-DT 為使用傳統決策樹演算法，可以觀察到 AFMA 在目標類別 U2R 的 Recall 由原先的 10.53%提升至 12.71%，證實 AFMA 能強化 U2R 此目標類別，但是 Normal 及 DoS 類別的 Recall 及整體 Accuracy 都較使用傳統決策樹演算法略為下降。

而與 AFMA 比較，MCFM 演算法在 Recall 的部分，除 R2L 及 Normal 類別表現略差之外，在 U2R、DOS 及 Probe 類別都較 AFMA 佳，而整體的 Accuracy 也由 92.61%提升至 92.66%，實驗結果證實 MCFM 演算法可改善 AFMA 只能對目標類別強化的缺點，對其他類別的分類效能也有提升的效果。

三、EIL演算法實驗

第二部分實驗之目的在證實 EIL 演算法能改良 IILA，進一步有效提升 U2R 類別及整體的分類效能。本實驗分類演算法同樣採用決策樹演算法，訓練資料集為 KDD 99 資料集的 10%訓練資料集樣本，特徵選取的部分參考文獻[20]，採用 ReliefF 演算法，選用權重值排序前 20 個特徵，實驗結果如表三。

表三 EIL 演算法與其他入侵偵測技術比較結果

類別	演算法 評估指標	C4.5 [10]	NB [10]	k-NN [10]	SVM [10]	KDDC up99 [10]	IILA-DT[8]	EIL-DT
Normal	Recall	98.13	90.00	95.77	98.01	**99.50**	98.80	98.87
	Precision	**74.89**	50.60	73.79	73.48	74.61	74.03	74.25
	F-measure	84.95	64.78	83.36	83.99	**85.28**	84.64	84.81
DoS	Recall	97.08	82.45	97.34	**97.47**	97.10	96.98	96.95
	Precision	99.93	98.00	99.66	99.87	99.88	99.87	**99.94**
	F-measure	98.49	89.55	98.49	**98.65**	98.47	98.40	98.42
Probe	Recall	**88.48**	78.01	81.93	86.68	83.30	85.79	82.38
	Precision	73.82	49.82	61.90	**77.36**	64.81	75.80	75.71
	F-measure	80.49	60.80	70.52	**81.75**	72.90	80.49	78.90
U2R	Recall	16.23	13.16	14.04	10.09	13.20	53.95	**55.70**
	Precision	2.62	2.79	3.53	54.76	**71.43**	15.09	13.86
	F-measure	4.51	4.60	5.64	17.04	22.28	**23.59**	22.20
R2L	Recall	3.38	5.42	5.06	3.36	8.40	8.18	**8.9**
	Precision	28.30	38.63	55.41	46.22	**98.84**	77.45	75.06
	F-measure	6.04	9.50	9.27	6.27	15.48	14.79	**15.92**
	Accuracy	92.23	79.80	91.96	92.47	**92.71**	92.46	92.52

資料來源：作者整理。

表三為 EIL 演算法與其他入侵偵測技術比較結果，粗體字代表最高的數值，底線則代表次高的數值。從比較表可看出，EIL 演算法與 IILA 相互比較，可看

[20]同註 7，頁 44。

出 EIL 演算法在 Normal、U2R 及 R2L 類別的 Recall 值都有提升。雖然文獻[21]所提出的 IILA，在少數重要類別(U2R 類別)已明顯優於其他方法。但是本研究提出的 EIL 演算法，在 U2R 及 R2L 類別的 Recall 值，分別可達到最高之 55.7%及 8.9%，均優於其他入侵偵測系統。另外對於多數類別的 DOS 與 Normal 均分別有 96.95%與 98.87%的 Recall，整體準確率亦可達 92.52%。由此可見，本研究所提出的 EIL 演算法可較其他方法更準確地偵測出 U2R 攻擊，而其他類別的分類效能也能維持一定的水準，或有效的改善。

四、EILBES實驗

本研究所提出的 EIL 演算法，經第二部分實驗證實，能成功強化 IILA 演算法對少數類別的分類效能，除了較 IILA 更加提升特定少數類別及新型態攻擊之偵測率外，也強化了其他類別的分類效能，並提升整體準確率，但是對於重要類別 U2R 的 Precision 及 F-measure 卻略為下降，對於入侵偵測系統而言，會產生較高的誤警率。

表四 EILBES 與其他入侵偵測技術比較結果

類別	演算法 評估指標	C4.5 [10]	NB [10]	k-NN [10]	SVM[10]	KDDCup 99 [10]	IILA 集成分類器[8]	EIL-DT	EILBES
Normal	Recall	98.13	90.00	95.77	98.01	**99.50**	99.04	98.87	99.01
	Precision	**74.89**	50.60	73.79	73.48	74.61	73.83	74.25	74.17
	F-measure	84.95	64.78	83.36	83.99	**85.28**	84.60	84.81	84.81
DoS	Recall	97.08	82.45	97.34	**97.47**	97.10	96.99	96.95	96.98
	Precision	99.93	98.00	99.66	99.87	99.88	99.88	**99.94**	99.91
	F-measure	98.49	89.55	98.49	**98.65**	98.47	98.42	98.42	98.43
Probe	Recall	**88.48**	78.01	81.93	86.68	83.30	80.68	82.38	81.82
	Precision	73.82	49.82	61.90	77.36	64.81	**77.73**	75.71	72.48
	F-measure	80.49	60.80	70.52	**81.75**	72.90	79.18	78.90	76.87
U2R	Recall	16.23	13.16	14.04	10.09	13.20	54.82	55.70	**57.01**
	Precision	2.62	2.79	3.53	54.76	**71.43**	27.23	13.86	29.61
	F-measure	4.51	4.60	5.64	17.04	22.28	36.39	22.20	**38.98**
R2L	Recall	3.38	5.42	5.06	3.36	8.40	8.46	**8.9**	8.37
	Precision	28.30	38.63	55.41	46.22	**98.84**	77.68	75.06	71.67
	F-measure	6.04	9.50	9.27	6.27	15.48	15.20	**15.92**	14.99
	G-mean	6.80	6.43	7.37	5.30	9.45	74.00	74.53	**75.47**
	Accuracy	92.23	79.80	91.96	92.47	**92.71**	92.53	92.52	92.53
	Cost	0.2426	0.4853	0.2459	0.2474	**0.2331**	0.2394	0.2388	0.2387

資料來源：作者整理。

[21]同註 7，頁 38。

本研究利用集成系統的優點，提出了基於 EIL 演算法集成系統來改善此一問題，為證實本研究所提出的 EILBES 可改善原 EIL 演算法之缺點，並進一步提升整體分類效能，進行第三部分的實驗，並與目前其他新型入侵偵測技術做比較，比較結果如表四。

表四中，粗體字代表最高的數值，底線則代表次高的數值。從比較表可看出， EIL 演算法雖然在少數重要類別(U2R 類別)已明顯優於其他方法，然而 EILBES 可將 Precision 由 13.86%提升至 29.61%，大大降低對於 U2R 類別的誤判率，且在 Recall 和 F-measure 分別可達到最高之 57.01%與 38.98%，均優於其他入侵偵測系統，由此可見 EILBES 可較其他方法更準確地偵測出 U2R 攻擊。

此外，本研究所提出的 EILBES 對屬於多數類別的 DOS 與 Normal 均分別有 96.98%與 99.01%的 Recall 值，與其他入侵偵測技術相似。而 EILBES 繼承 IILA 的優點，利用取樣策略僅使用少數的訓練樣本，因此在計算效能上較其他方法來得好；再加上 EILBES 在大部分類別的分類效能均優於 EIL 演算法，而整體準確率 92.53%與成本 0.2387 亦優於 EIL 演算法。從以上的實驗結果與分析比較，可證實 EILBES 能強化 EIL 演算法，降低入侵偵測系統誤判率，更可以進一步提升入侵偵測系統的整體效能。

結論與未來研究方向

身處資訊如此發達的時代，網路使用者除了本身應具備一定的資訊安全常識外，安全的使用環境更是極其重要，不管是民間公司或政府機關，對於目前的網路環境，都面臨到最大威脅與考驗，入侵偵測系統就是其中一道重要的防線。入侵偵測系統相關研究很多，但是仍存在著一些困難待克服，例如：少數攻擊類別偵測率不佳等。因此，本研究提出 EIL 演算法與 EILBES 來解決這些問題，經由實驗證實可成功改善網路異常入侵偵測分類效能，本研究之效益分析如下：

一、KFCR 演算法能篩選出較佳訓練資料，避免 MCFM 演算法在錯誤回饋時將較差訓練資料回饋，降低分類效能。

二、MCFM 演算法可改善 AFMA 演算法僅對特定類別的分類效能提升的缺點，除了對少數類別外，對其他類別的分類效能也有強化的效果。

三、EIL 演算法整合本研究提出的 KFCR 及 MCFM 演算法，並成功改良 IILA 演算法，對少數類別及整體分類效能均有強化效果。

四、EILBES 可提升 U2R 攻擊類別的 Recall 達 57.01%，本項結果也優於其他入侵偵測系統，證實可有效偵測少數重要的網路異常入侵行為，對於其他類

別的分類效能也有一定的水準，成功提升入侵偵測系統效能。

本研究所提出的演算法仍有需要加強的地方，例如：對於 R2L 類別之分類效能仍未能有效提升與分類效率不佳等問題。因此，在未來的發展上，有以下三個方向值得進一步研究：

一、雜訊去除

加入雜訊去除部分，將 KFCR 演算法進行改良，可進一步結合分群(Cluster)演算法，更精確的去除雜訊，相信可提升整體的分類效能。

二、整體學習

單一分類器能達到的分類效果有限，若能增加基本分類器，且對於各分類模型賦予各別不同的權重，並在最後推論時根據此一權重值來實施權重投票(Weighted Voting)，應可獲得更佳的分類效果。

三、資料整合

本論文之演算法運用於單一種資料集，未來可結合各式資安設備，如防火牆、誘捕系統(Honeypot)和防毒系統等，建立各別的分類模型，並做最後的集成推論，相信有助於分類效能提升。

參考文獻

一、詹益東，〈網路異常入侵偵測分類效能改善方法〉(桃園：國防大學中正理工學院資訊科學所碩士論文，2010 年)。

二、潘致誠，〈強健式網路入侵偵測演算法則之研究〉(桃園：國防大學中正理工學院資訊科學所碩士論文，2009 年)。

三、葉志飛、文益民、呂寶糧，〈不平衡分類問題研究綜述〉《智能系統學報》，第 4 卷第 2 期，2009 年。

四、尹相志，《Microsoft SQL Server 2005 資料採礦聖經》(台北：學貫行銷股份有限公司)，2007 年。

五、張琦、吳斌、王柏，〈非平衡數據訓練方法概述〉《計算機科學》，第 32 卷第 10 期，2005 年。

六、周加恩，〈網路安全偵測之分類效能提昇〉(桃園：國防大學中正理工學院資訊工程所碩士論文，2012 年)。

七、曾鴻麟，〈利用取樣技術提升網路入侵偵測效能之研究〉《陸軍通資半年刊》，第 124 期，2015 年 9 月。

八、Doyle, J., Kohane, I., Long W., Shrobe, H., and Peter, S., “Event Recognition Beyond Signature and Anomaly,” Proceedings of the 2001 IEEE, Workshop on

Information Assurance and Security, United States Military Academy, West Point, NY, 2001.

九、Tan, P. N., Steinbach, M., and Kumar, V., Introduction to Data Mining, (U.S.A:MORGAN KAUFMANN PUBLISHERS, 2006).

十、Robi Polikar, “Ensemble based systems in decision making,” IEEE Circuits and Systems Magazine, Vol. 6, 2006.

十一、Haibo He, and Edwardo A. Garcia, “Learning from Imbalanced Data,” Knowledge and Data Engineering, vol. 21, no. 9, 2009.

十二、Abu H. M Kamal, Xingquan Zhu, Abhijit Pandya and Sam Hsu, “Feature Selection with Biased Sample Distributions,” IEEE IRI 2009, 2009.

十三、N.V. Chawla, K.W. Bowyer, L.O. Hall, and W.P. Kegelmeyer, “SMOTE: Synthetic Minority Over-Sampling Technique,” Artificial Intelligence Research, Vol. 16, 2002.

十四、Naeem Seliya, Zhiwei Xu, and Taghi M. Khoshgoftaar, “Addressing Class Imbalance in Non-Binary Classification Problems,” 20th IEEE International Conference on Tools with Artificial Intelligence, 2008.

十五、http://www.cs.waikato.ac.nz/ml/weka/, 2011/4/20.

十六、http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html, 2011/4/20.