應用有效的群集分析機制於入侵偵測系統之研究

林東森、曹偉駿

E-mail: 9222744@mail.dyu.edu.tw

摘 要

近年來，隨著網際網路的盛行、電腦使用的普及與網路技術發展的成熟，使得網際網路成為商業交易的媒介，吸引了社會大眾的關注。但相對的也造成駭客攻擊事件及網路犯罪行為不斷的出現於新聞媒體報導中，遭受入侵攻擊所造成的潛在危害不僅難以估計，更暴露出電腦系統本身存在的安全問題。入侵偵測系統就是為了防禦及偵測駭客入侵的攻擊行為，而且駭客的入侵攻擊行為也可經由網站之網頁系統記錄檔中發現；若能分析網頁的系統記錄檔，將有助於入侵偵測系統的建置。因此，本研究主要採用分群法與分類法對網頁系統記錄檔進行分析，以區分出正常的使用者行為及異常的入侵攻擊行為。雖然分群法可以對龐大的網頁系統記錄檔進行群集分析，但是一般的分群演算法皆需要設定已知的群數，才能進行分群運算，而且已知的群數是很難決定的。假使能藉由分群效度指標的輔助，自動評估分群結果的好壞，將可獲得較佳的分群結果。當有新的網頁系統記錄檔增加時，所有的分群工作便要重新再來，若能採用分類法的優點，將可處理日益漸增的網頁系統記錄檔。 本研究基於以上的考量，整合了較快速的分群演算法(Modified mrFCM)與評估分群結果優劣的分群效度指標(指標)來解決群集分析的問題，並進一步使用Modified K-NN分類法來處理日益漸增的網頁系統記錄檔，以作為建置入侵偵測系統的參考依據。此外，本研究亦有開發成實際的系統，經由真實的網頁系統記錄檔進行分群與分類分析，以顯示出本研究所提出的方法確實能達到預期的成效。

關鍵詞 : 入侵偵測系統、分群法、分群效度指標、分類法。

目錄

參考文獻

[1] 李志明，影像最佳類別數目之研究，國立中央大學碩士論文，民國90年6月。

[2] 范義明，Linux作業系統下異常偵測之研究，大葉大學碩士論文，民國91年6月。

[3] 許文豪，圖形辨識概述與實作，國立清華大學碩士論文，民國89年7月。

[4] 黃景彰，資訊安全-電子商務之基礎，華泰文化事業公司，民國90年6月。

[5] 賴溪松、葉育斌，資訊安全入門，全華科技圖書，民國90年6月。

[6] 譚嘉慧，模糊分類適切性分析，中原大學碩士論文，民國89年6月。

[7] J. C. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms, Plenum Press, New York, 1981.

[8] R. H. Charles, Cluster analysis for researchers, 茂昌圖書有限公司, 1985.

[9] T. W. Cheng, D. B. Goldgof, and L. O. Hall, Fast Fuzzy Clustering, Fuzzy Sets and Systems, Vol. 93, pp. 49-56, 1998.

[10] V. Cherkassky, and F. Mulier, Learning from Data : Concepts, theory, and methods. New York : Wiley, 1998.

[11] Y. Fukayama and M. Sugeno, A New Method of Choosing the Number of Cluster for the Fuzzy c-mean Method, Proceedings of 5th Fuzzy Systems Symposium, pp. 247-250, 1989.

[12] K. Fukunaga, Introduction to Statistical Pattern Recognition, Academic Press, 1990.

[13] J. S. Jang, C. T. Sun, and E. Mizutani, Neuro-Fuzzy and Soft Computing, Prentice Hall, New Jersey, 1997.

[14] M. F. Jiang, S. S. Tseng, and C. M. Su, Two-Phase Clustering Process for Outliers Detection, Pattern Recognition Letters, Vol. 22, pp. 691-700, 2001.

[15] R. A. Johnson, and D. W. Wichern, Applied Multivariate Statistical Analysis, Prentice-Hall, New Jersey, 1998.

[16] D. J. Kim, Y. W. Park, and D. J. Park, A Novel Validity Index for Determination of the Optimal Number of Clusters, IEICE Transactions on

Information and Systems Society, Vol. E84-D, No. 2, pp. 281-285, 2001.
[17] NetCraft http://www.netcraft.com/ [18] N. R. Pal and J. C. Bezdek, On Cluster Validity for the Fuzzy c-means Model, IEEE Transactions on Fuzzy Systems, Vol. 3, No. 3, 1995.
[19] N. R. Pal and J. C. Bezdek, Correspondence to "On Cluster Validity for the Fuzzy c-means Model", IEEE Transactions on Fuzzy Systems, Vol. 5, No. 1, 1997.
[20] Superscan http://www.foundstone.com/ [21] A. Sundaram, An Introduction to Intrusion Detection, ACM Crossroads Student Magazine. http://www.acm.org/crossroads/xrds2-4/intrus.html [22] X. L. Xie, and G. Beni, A Validity Measure for Fuzzy Clustering, IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 841-847, 1991.
[23] L. A. Zadeh, Fuzzy Sets, Information Control, Vol. 8, pp. 338-353, 1965.