

Learning-Based Intrusion Detection Scheme for Wireless Local Area Networks

楊敦仁、曹偉駿

E-mail: 9806146@mail.dyu.edu.tw

ABSTRACT

Since the technology of wireless local networks were invented, the character of data transmitting without being restricted by any physical media can let people access and share network resources anytime. Although the wireless infrastructure brings much convenience to us, at the same time, a large number of information is secret exposed. Hence, hackers can wiretap the transmitted data and embezzle the resources of wireless facilities, so that intrusion detection systems become indispensable roles wireless local networks. However, current intrusion detection systems arise too much false-alarm and false-negative with the result that system administrators should deeply concern about whether the alarm is useless and notice the effectiveness of rule base. Therefore, our research addresses this issue by integrating fuzzy association rules into the linear discriminant analysis (LDA) to construct a hybrid intrusion detection scheme. By employing misuse detection, we implement LDA to find out the unknown attacks which were hidden among the regular behaviors, then trace their attack patterns and characteristics by using the fuzzy association rules, and further automatically add the rules into the rule base to achieve the goal of self-learning functionality, such that it can increase the detecting rate of intrusion detection system and enhance the updating efficiency of rule base. Finally, an intrusion detection system was implemented to demonstrate the feasibility of our proposed scheme.

Keywords : intrusion detection system、discriminant analysis、fuzzy association rules、wireless local area networks

Table of Contents

中文摘要	iii
英文摘要	iv
誌謝辭	vi
內容目錄	vii
表目錄	ix
圖目錄	x
第一章 緒論	1
第一節 研究背景與動機	1
第二節 研究目的	2
第三節 研究限制	3
第四節 研究流程	3
第五節 論文架構	5
第二章 文獻探討	6
第一節 現行無線區域網路安全議題	6
第二節 入侵偵測系統探討	10
第三節 資料探勘技術	15
第三章 學習導向之無線區域網路入侵偵測機制	23
第一節 稽核資料選取與量化	24
第二節 線型判別分析	26
第三節 模糊關聯法則分析	29
第四節 偵測比對流程	35
第四章 實驗設計與系統測試	36
第一節 實驗軟硬體環境	36
第二節 系統介面介紹	37
第三節 系統測試	39
第四節 實驗結果與分析	44
第五章 結論與未來發展	49
參考文獻	51

REFERENCES

- 一、中文部份台灣電腦網路危機處理?協調中心, (2003), 802.11無線網路安全白皮書[線上資料], 來源: <http://www.cert.org.tw/> 16[2009, June 19]。李駿偉、田筱榮、黃世昆, (2002), 入侵偵測分析方法評估與比較, 資訊安全通訊。第八卷第二期8(2), 21-37。曹偉駿、梁成揚, (2008), 基於資料挖掘技術之Linux無線區域網路入侵偵測系統, 第18屆資訊安全會議, 179-192。
- 二、英文部份Asaka, M., Onabuta, T., Inoue, T., Okazawa, S., & Goto, S. (2001). A new intrusion detection method based on discriminant analysis. *IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS E SERIES D*, pp.570-577.Agrawal, R., & Srikant, R. (1994). Fast algorithms for mining association rules. *Proceedings 20th Int. Conf. Very Large Data Bases*.Balazinska, M., & Castro, P. (2003). Characterizing mobility and network usage in a corporate wireless local – area network. In J. Pieprzyk & H. Ghodosi (Eds.). *Proceedings of the 1st international conference on Mobile systems. applications and services*, (pp. 303 – 316), New York: Springer – Verlag.Boncella, R. J. (2006). *Wireless Threats and Attacks. Handbook of information security*.Boudriga, N., & Obaidat, M. S. (2006). Mobility, sensing, and security management in wireless ad hoc sensor systems. *Computers & Electrical Engineering*, 32(1 – 3), 266 – 276.Choi, Y. B., Muller, J. Kopek, C. V., & Makarsky, J. M. (2006) . Corporate Wireless LAN Security:Threats and an Effective Security Assessment Framework for Wireless Information Assurance. *International Journal of Mobile Communications*, 4(3), 266 – 290.Daniels, T., & Spafford, E. H. (1999). Identification of host audit data to detect attacks on low – level IP vulnerabilities. *Journal of Computer Security*, 7(1), 3 – 35.Debar, H., & Viinikka, J. (2005). *Intrusion Detection: Introduction to Intrusion Detection and Security Information Management. Foundations of Security Analysis and Design III*, Vol. 3665, pp. 207-236.Ettercap. (2005), sourceforge.net, [online] Available: <http://ettercap.sourceforge.net/index.php/>[2009, April 15].Fake AP Project. (2005), blackalchemy.to, [online] Available: <http://www.blackalchemy.to/project/fakeap/>[2009, June 23] .Florez, G., Bridges, S. A., & Vaughn, R. B. (2002). An improved algorithm for fuzzy data mining for intrusion detection. In L. Xu & L. Korba (Eds.), *Proceedings of the North American Fuzzy Information Processing Society Conference*, (pp. 457-462) , New York: Springer-Verlag.Gill, R., Smith, J., & Clark, A. (2006). Specification- Based Intrusion Detection in WLANs, *Proceedings of 22nd Annual Computer Security Applications Conference*, Miami.Guan, Y., Ghorbani, A. A., & Belacel, N. (2003). Y – means: A clustering method for intrusion detection. In D.T. Lee & B.S. Lin (Eds.). *Proceedings of Canadian Conference on Electrical and Computer Engineering*, (pp. 1 – 4), New Jersey: IEEE.Hall, J., Barbeau, M., & Kranakis, E. (2003). Detection of transient in radio frequency fingerprinting using phase characteristics of signals, *Proceedings of the 3rd IASTED International Conference on Wireless and Optical Communications (WOC 2003)*, pages 13 – 18, Banff, Alberta, Canada, July. ACTA Press.Heady, R., Luger, G. Maccabe, A., & Servilla, M. (1990). The architecture of a network level intrusion detection system. Technical report CS90 – 20, University of New Mexico: Department of Computer Science.Hu, Y. C., Chen, R. S., & Tzeng, G.H. (2003). Discovering fuzzy association rules using fuzzy partition methods. *Knowledge-Based Systems*, 16(3), 137-147.Hossain, M. (2002). Integrating association rule mining and decision tree learning for network intrusion detection: a preliminary investigation. In I.F. Akyildiz, J.Y.B. Lin, & R. Jain (Eds.), *Proceedings of the International Conference on Information Systems, Analysis and Synthesis*, (pp. 65-70), New Orleans: IEEE.Iheagwara, C., Blyth, A., & Bennett, M. (2005) Architectural and Functional Issues in Systems Requirements Specifications for Wireless Intrusion Detection Systems Implementation. *Proceedings of the Systems Communications*, (pp. 434-441).Jain, A. K., Murty, M. N., & Flynn, P. J. (1999). Data clustering: a review. *ACM Computing Surveys*, 31(3), 264-323.Jha, S., & Hassan, M. (2002). Building agents for rule – based intrusion detection system. *Computer Communications*, 25(15), 1366-1373.Khoshgoftaar, T. M., Nath, S. V., Zhong, S., & Seliya, N. (2005). A clustering approach to wireless network intrusion detection. In J. Crowcroft (Ed.), *Proceedings of International Conference on Tools with Artificial Intelligence*, (pp. 190 – 196), London: ACM.Lazarevic, A., Ertöz, L., Kumar, V., Ozgur, A., & Srivastava, J. (2003). A comparative study of anomaly detection schemes in network intrusion detection, *Proceedings of Third SIAM Conference on Data Mining*.Lee, W., Stolfo, S. J., & Mok, K. W. (1999). A data mining framework for building intrusion detection models. In P. Druschel & M.F. Kaashoek (Eds.), *Proceedings of the 1999 IEEE Symposium on Security and Privacy*, 120-132, New York: IEEE.Lei, J., Fu, X., Hogrefe, D., & Tan, J. (2007). Comparative Studies on Authentication and Key Exchange Methods for 802.11 Wireless LAN. *Computers & Security*, 26(5), pp. 401-409.Liu, Y., Tian, D., & Li, B. (2006). A Wireless Intrusion Detection Method Based on Dynamic Growing Neural Network. *Proceedings of the First International Multi-Symposiums on Computer and Computational Sciences*. 2, 611- 615.Luo, J., Bridges, S., & Vaughn, R. B. (2001). Fuzzy frequent episodes for real – time intrusion detection. In D. Maughan & N.H. Vaidya (Eds.), *Proceedings of IEEE International Conference on Fuzzy Systems*, (pp. 368-371), Atlanta: IEEE.Ouyang, Y. C., Chang, R. L., & Chiu, J. H. (2003). A New Security Key Exchange Channel for 802.11 WLANs. *Proceedings of 37th Annual International Carnahan Conference on Security Technology*.Pacha, A., & Park, J. M. (2007). An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks*, 51, 3448-3470.Raya, M., Hubaux, J. P., & Aad, I. (2004). DOMINO: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots. *ACM MobiSys*, June, Boston, USA.Sobh, T. S. (2006). Wired and wireless intrusion detection system: classifications, good characteristics and state – of – the – art. *Computer Standards & Interfaces*, 28(6), 670-694.Stearley, J. (2004). Towards informatic analysis of syslogs. In H. Krawczyk (Eds.), *Proceedings of the IEEE International Conference on Cluster Computing*, (pp. 309 – 318), San Francisco: IEEE.Tajbakhsh, A., Rahmati, M., & Mirzaei, A. (2008). Intrusion detection using fuzzy association rules. *Applied Soft Computing*, 9(2), 462-469.Tsaur, W. J., & Yu, C. C. (2006). Design and Implementation of Highly Accurate Hierarchical Clustering Algorithm for Intrusion Detection. *Journal of Internet Technology*, Volume 7(2), 177-183.Tsaur, W. J., & Shieh, Y. C. (2003). Constructing fuzzy association rules for intrusion detection systems. In N. Koblitz (Eds.), *Proceedings of the 2003 National Computer Symposium*, (pp. 1256-1263), New York: Springer-Verlag.Void11. (2005), wirelessdefence.org, [Online] Available:

<http://wirelessdefence.org/Contents/Void11Main.htm> [2009, May 12]Wang, S., Tao, R., Wang Y., & Zhang, J. (2003). WLAN ONLINE and It's Security Problems. Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 241- 244.Wall, D., Kanclirz, J. J., Jing, Y., Faircloth, J., & Barrett, J. (2004). Managing and Securing a Cisco SWAN, SYNGRESS.Wong, W. T., & Lai, C. Y. (2006). Identifying Important Feature for Intrusion Detection Using Discriminant Analysis and Support Vector Machine. Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16. August.