Learning-Based Intrusion Detection Scheme for Wireless Local Area Networks

Yuen-Den Yang, Pei-Chun Tsao

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  總論................................ 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


