บทคัดย่อ

ในปัจจุบันระบบเครือข่ายคอมพิวเตอร์มีการเติบโตอย่างรวดเร็ว ทำให้ระบบตรวจจับการบุกรุกกลายเป็นส่วนสำคัญส่วนหนึ่งของระบบเครือข่าย ในระบบตรวจจับการบุกรุกบางระบบจะอาศัยพฤติกรรมการใช้งานเครือข่ายแบบปกติเป็นตัวตรวจจับพฤติกรรมที่แปลกปลอม แต่ในบางระบบก็จะอาศัยการจดจำรูปแบบการบุกรุก ระบบตรวจจับการบุกรุกที่พัฒนาในปัจจุบันนี้มีการประยุกต์ใช้ปัญญาประดิษฐ์กันอย่างกว้างขวางเพื่อเพิ่มประสิทธิภาพในการตรวจจับรูปแบบการบุกรุกใหม่ๆ ได้

งานวิจัยฉบับนี้นำเสนอระบบตรวจจับการบุกรุกโดยใช้ระบบ LCS โดยเราพัฒนาส่วนของการแบ่งระดับค่าความผิดปกติของข้อมูลโดยใช้แผนภาพ Self-Organizing Map โดยการเข้ารหัส 2 บิต ขึ้นอยู่กับค่าความเบี่ยงเบนจากพฤติกรรมการใช้งานปกติ เราได้ทำการทดลองกับข้อมูล FTP-Only และข้อมูลที่เก็บมาจากมหาวิทยาลัยรามคำแหง จากผลการทดลองแสดงให้เห็นว่าระบบที่เราได้นำเสนอมีประสิทธิภาพดีกว่าระบบ LCS เดิมและระบบจักรกลเรียนรู้อื่นๆ อีก 12 ระบบ

Abstract

Nowadays, as interconnections among computer systems grow rapidly, Intrusion Detection Systems (IDSs) play an important role of network security. Some systems are anomaly based and others are signature based. However, no detection system can catch all types of intrusions. At the moment most of the researchers are interested in improving intrusion detection which includes artificial intelligence.

In this research, we propose intrusion detection system using Learning Classifier System –LCS. We extends work in the area by applying the Self-Organizing Map (SOM) for creating the new input string by 2-bit encoding rely on degree of deviation of normal behaviour. The performance of systems is investigated under an FTP-only dataset and data from Ramkhamhaeng University. It is shown that the proposed system is able to perform significantly better than the conventional XCS and twelve ML algorithms.