เบญจวรรณ สุขพัฒนศรีกุล 2552: การตรวจจับความผิดปกติของทราฟฟิกและลักษณะเครือข่ายเพื่อจัดกลุ่มความผิดปกติของทราฟฟิก กรณีศึกษา: บริษัท ทีโอที จำกัด (มหาชน) ปริญญาวิศวกรรมศาสตรมหาบัณฑิต (วิศวกรรมคอมพิวเตอร์) สาขาวิศวกรรมคอมพิวเตอร์ ภาควิชาวิศวกรรมคอมพิวเตอร์ อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก: รองศาสตราจารย์ศิริพร อ่องรุ่งเรือง, M.S. 85 หน้า

ระบบเครือข่ายขององค์กรมีความเสี่ยงสูงที่จะถูกโจมตีหรือถูกการก่อกวนอย่างไม่ได้คาดคิดมาก่อน แม้ว่าจะมีการใช้งานระบบความปลอดภัยที่เหมาะสมอยู่แล้วก็ตาม วัตถุประสงค์ของโครงงานการค้นคว้าวิจัยนี้จะใช้เทคนิคการทำเหมืองข้อมูลด้วยเทคนิคต่างๆ ซึ่งประกอบด้วย อัลกอริทึม sIB RandomFlatClustering FarthestFirst FilteredClusterer และ K-Means เพื่อนำมาจัดกลุ่มข้อมูลประเภท TCP/IP แพ็กเก็ต และทำการเปรียบเทียบผลการจัดกลุ่มของแต่ละเทคนิคเพื่อหาอัลกอริทึมที่เหมาะสมที่สุดสำหรับใช้ตรวจจับความผิดปกติของทราฟฟิก ผลลัพธ์ของการจัดกลุ่มข้อมูลจะสามารถนำไปสร้างกฎใหม่เพื่อนำใช้ในเครื่องมือที่ใช้ในการตรวจจับความผิดปกติได้

221408

Benjawan Sukpattanasrikul 2009: Traffic Anomaly Detection and Characterization to Cluster Traffic Anomalies Case Study: TOT Public Company Limited. Master of Engineering (Computer Engineering), Major Field: Computer Engineering, Department of Computer Engineering. Thesis Advisor: Associate Professor Siriporn Ongroongrueng, M.S. 85 pages.

Network System of an organization has a high risk to be unexpectedly attacked or disturbed even though an appropriate security system has been provided. The objective of this research project is to apply various clustering data mining techniques, sIB, RandomFlatClustering, FarthestFirst, FilteredClusterer and K-Means to perform TCP/IP packet clustering and compare the anomaly detection efficiency of each technique to find out which algorithm is the most appropriate one for detection of traffic anomaly. The clustering result has been used to create new rules for detection software tool to improve its detection capability.