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.

__________________________ __________________________ ___ / ___ / ___

Student’s signature Thesis Advisor’s signature