

TELKOM UNIVERSITY

Abstract

School of Computing

The Graduate School

Master of Engineering

Semi – supervised Method for Anomaly Intrusion Detection System

by Sofy Fitriani

Nowadays, number of attacks against computer networks are increasing which make security becomes an important issue in this system. Because of that, the system needs to maintain the security of computer networks. One of them is using Intrusion Detection System (IDS). The type of attacks usually has a different rhythm with normal traffic. Therefore, the research conducted this anomaly-based intrusion. This study uses a machine learning method, ie semi-supervised. This method is a combination of supervised and unsupervised. Typically, detection techniques is using single classifier such as supervised and unsupervised learning. However, disadvantages supervised method is the method does not work well on the unknown attack and time consuming to recognize the attack. Detection accuracy becomes worse when faced with the unknown attacks. Unsupervised method showed no significant difference with supervised methods in the detection accuracy and had a high false positives. In semi-supervised IDS (SS-IDS) is using proposed feature selection and help with filtering multicollinearity in preprocessing to get a better training phase. The result showed that proposed method got low false positive 18.75% and high accuracy 89.02%.

Keywords : Computer Network, Intrusion Detection System, Semi-supervised, Machine Learning, Network Security