Thesis Title	Strengthening Intrusion Detection System for Adversarial Attacks: Improved Handling of Imbalance Classification Problem
Author	Chutipon Pimsarn
Degree	Master of Science (Information Technology)
Advisor	Assoc. Prof. Wg. Cdr. Tossapon Boongoen, Ph. D.
Co-Advisor	Assoc. Prof. Natthakan Iam-on, Ph. D.

ABSTRACT

A network-based intrusion system or NIDS is the best defense mechanism, often sup-optimal for detecting an unseen malicious pattern. In response, many studies have attempted to promote NIDS that uses machine learning to improve their ability to recognize an opponent's attack. According to this research line, the current work focuses on non-payload connections at the TCP stack level, which is generalized and applicable to different network applications. As a complement to the recently published investigation that searches for the most informative feature space for classifying obfuscated connections, the problem of class imbalance is examined herein. Especially, a multiple-clustering-based undersampling framework is proposed to determine the set of cluster centroids that best represent the majority class to reduce par size to be equal to the minority. Initially, a pool of centroids is created using ensemble clustering to obtain a group of precise and diverse groupings. Then select the last representative from this group. Three different objective functions are formed for this optimization-driven process, thus leading to three variants of FF-Majority, FF-Minority, and FF-Overall. Based on a detailed assessment of the published dataset, four classification models, and different settings, these new methods show better predictive performance than baseline

data: the single-clustering undersampling counterpart and state-of-the-art techniques. Parameter analysis and implications for analyzing an extreme case are also guidelines for future applications.

Keywords: Intrusion detection system, Adversarial attack, Machine learning, Imbalance classification, Data clustering