Initial Literature Review for IDS System

11 October 2016

1 Introduction

In total three papers are reviewed to compare the advantages and disadvantages of different machine learning techniques in the use for Intrusion Detection and Intrusion Prevention system.

The papers under reviewing are listed as follows:

- Thapngam, Shui and Wanlei [1]
- Aghdam & Kabiri, 2016 [2]
- Fernandes, et al. [3]

2 Related Work

Network intrusion detection gained a lot of attention from the security expert. Intrusion detection system has been designed for the purpose detecting attack and comprises of detection method that can be anomaly based or it can be signature based.

2.1 DDoS Detection using LDA

In this paper[1], authors propose to use the supervised learning model based on Linear Discriminant Analysis (LDA) from the pattern behaviour of traffic sources by observing packet arrivals. The learnt model is then used to discriminate traffic flows among DDoS attack sources and legitimate users.

2.2 Feature Selection using ACO

In this paper, authors has proposed an intrusion detection system that its features are optimally selected using Ant Colony Optimization (ACO) [2]. The purpose of this study is to identify important features in building an intrusion detection system such that they are computationally efficient and effective. The proposed method outperforms previous approaches through the extensive experimental results on the KDD Cup 99 and NSL-KDD intrusion detection benchmark data sets by providing higher accuracy in detecting intrusion attempts and lower false alarm with reduced number of features.

2.3 Network Anomaly Detection by PCA + ACO

Aiming an automated management to detect and prevent potential problems, the authors present and compare two novel anomaly detection mechanisms based on statistical procedure Principal Component Analysis and the Ant Colony Optimization metaheuristic [3]. These methods generate a traffic profile, called Digital Signature of Network Segment using Flow analysis (DSNSF), which is adopted as normal network behavior. Then, this signature is compared with the real network traffic by using a modification of the Dynamic Time Warping metric in order to recognize anomalous events.

3 Proposed Method

Anomaly-based IDS such as [1] usually deals with statistical analysis and pattern recognition problems. Supervised learning approach for the detection method finds the relationship between the feature and its class. These DDoS detection method highly depends on the quality of the input features. Therefore, irrelevant, redundant, and noisy features must be eliminated before applying supervised algorithm.

This can be done by feature selection method, as did in [2]. Feature selection means selecting a useful subset from all features. So one must not transform input features into another set of features in feature selection. Therefore, their method suffers from high computational expense due to large amount of network traffic data and high dimensional feature space.

To summary, the limitations of previous work (hence the contributions of proposed method) are:

LDA for DDoS Detection [1] :

- No feature selection
- No feature dimensionality reduction

ACO for Feature Selection [2] :

- No feature dimensionality reduction

PCA + ACO for Network Anomaly Detection [3] :

- PCA and ACO are mainly used to generate Digital Signature of Network Segment for the purpose of anomaly detection in later process
- Performance is rather limited as the authors only used simple adaptive Dynamic Time Warping method for anomaly detection
- The proposed method improved the results by using state-of-the-art neural network classifier

References

[1] Thapngam, Theerasak, Shui Yu, and Wanlei Zhou. "DDoS discrimination by linear discriminant analysis (LDA)." *Computing, Networking and Communications (ICNC), 2012 International Conference on.* IEEE, 2012.

[2] Aghdam, Mehdi Hosseinzadeh, and Peyman Kabiri. "Feature selection for intrusion detection system using ant colony optimization." *International Journal of Network Security* 18.3 (2016): 420-432.

[3] Fernandes, Gilberto, et al. "Network anomaly detection using IP flows with Principal Component Analysis and Ant Colony Optimization." *Journal of Network and Computer Applications* 64 (2016): 1-11.