Design of an Intrusion Detection System for Unknown-attacks based on Bio-inspired Algorithms

Kyung-min Kim† HakJu Kim† Kwangjo Kim†

† School of Computing, KAIST
KAIST 291, Daehak-ro, Yuseong-gu, Daejeon 34141, Republic of Korea
{saza12345, ndemian, kkj}@kaist.ac.kr

Abstract Signature-based Intrusion Detection System (IDS) can detect only known attacks that have signatures. As new unknown-attacks are appearing continuously, the detection of unknown-attacks has become the essential part of IDS. This paper presents a novel design of IDS by combining two existing bio-inspired machine learning algorithms; Artificial Immune System (AIS) and Ant Clustering Algorithm (ACA), and evaluates the pros and cons of the approach. In our approach, after ACA makes clusters by using unsupervised learning, AIS categorizes the network traffic to self and non-self as normal and abnormal profiles, respectively. Our design presents better performance than other existing similar design.

1 Introduction

Intrusion Detection System (IDS) monitors network traffic and detects users' abnormal or malicious activities. Two well-known detection types of IDS are Signature-based detection and Anomaly-based detection. Signature-based detection compares an input traffic with distinctive signatures of known attacks, and makes decision whether the input traffic is a real attack or not . Anomaly-based detection concentrates on making profiles of normal behaviors, and considers a traffic with an abnormal behavior as an attack.

As the architecture of networks are diversified, new unknown-attacks will be emerged very fast. Because Signature-based detection uses pattern matching technique to detect attacks, the detection type cannot detect unknown-attacks which don't have signatures. In contrast, Anomaly-based detection concentrates abnormal activities of a system. Thus, any unknown-attacks violating the normal profile of a system can be detected using Anomaly-based detection.

Many Anomaly-based detection algorithms[1][2] have been proposed to detect unknown-attacks. Artificial Immune System (AIS) [3] and Ant Clustering Algorithm (ACA) [2][4] are members of bio-inspired machine learning algorithms used to implement Anomaly-based detection. AIS is inspired by human immune system and has capability to differentiate normal and abnormal states. ACA is inspired by the movements of ants and makes clusters by using simple

movements of a number of artificial ants. In this paper, we combine these two algorithms and propose a novel IDS architecture.

The remainder of the paper is organized as follows: In Section 2, we briefly review some related work. We present the proposed IDS in Section 3. Our comparison on other existing methods is followed in Section 4. Summary and future work are stated in Section 5.

2 Background

In this section, we discuss briefly some related work.

2.1 Intrusion Detection System

Intrusion Detection is a kind of functions that analyzes and detects malicious attacks or abnormal behaviors on certain hosts or networks [5].

IDS implements intrusion detection techniques to check traffic/data to detect intrusion. IDS can be classified into Network IDS (NIDS) and Host IDS (HIDS) by the location of IDS sensors. IDS sensors of NIDS are located in network routers to monitor entire traffic of the network and IDS sensors of HIDS are located in a target host.

Among many measures used to evaluate the performance of an IDS, Detection Rate (DR) and False Positive Rate (FPR) are the most significant measures. DR is defined as the number of intrusion instances detected by the system divided by the total number of intrusion instances present in the test set. FPR is defined as the number of normal patterns classified as attacks divided by the total number of normal patterns [6]. A good IDS requires higher DR and lower FPR.

2.2 KDD Cup 99 Dataset

KDD Cup 99 Dataset is a version of DARPA 1998 Intrusion Detection Evaluation Program. A standard set of data to be audited, which includes a wide variety of intrusions simulated in a military network environment, has been rigorously suggested. The 1999 KDD intrusion detection contest uses KDD Cup 99 Dataset [7].

KDD Cup 99 Dataset has about 18 million of packet headers. The dataset is composed of 5 types of packet; normal, probe, DoS, U2R, and R2L. The types are described as follows:

- Normal : not attack
- Probe : surveillance and other probing (*e.g.*, port scanning)
- DoS : denial-of-service (*e.g.*, syn flood attack)
- U2R : unauthorized access to local superuser/root privileges (*e.g.*, buffer overflow attack)
- R2L : unauthorized access from a remote machine (*e.g.*, guessing password)

The packet distribution of KDD Cup 99 Dataset is presented in Table 1 as below:

Table 1 Packet distribution of KDD Cup 99 Dataset

Type	# of packets	Proportion (%)
Normal	80,767	26.0
Probe	5,356	1.7
DoS	223,488	71.9
U2R	228	0.0
R2L	1,376	0.4
Total	311,029	100

2.3 Unknown-attack Detection

Unknown-attack is a type of attacks that IDS has no knowledge about the previous known attack. Because the signature of unknown-attack is unknown, Signature-based detection method cannot detect unknown-attacks. In contrast, Anomaly-based detection method is capable of detecting unknown-attacks. Thus, Anomaly-based detection is mainly used in unknown-attack detection.

The performance of Anomaly-based detection relies highly on the effectiveness of building normal behavior profile. Currently, a variety of machine learning techniques and data mining techniques are used to make the effective and robust normal behavior profile [1][2].

2.4 Artificial Immune System (AIS)

Human Immune System (HIS) defends the human body against harmful foreign cells, including previously unseen foreign cells using lymphocyte cells. The foreign cells are called antigens, such as bacteria and viruses [3]. AIS is designed for the computational system and inspired by HIS [1]. AIS has the capability to differentiate between the 'self' (cells that are owned by the system) and 'non-self' (foreign entities to the system).

The HIS employs a negative selection process to generate mature immune system cells called as T-cells. Forrest, *et al.* [8] proposed a negative selection algorithm, inspired by HIS, for Anomaly-based detection. The process allows the detection of the regardless of previously unseen attacks any knowledge.

The algorithm consists of three phases. defining self, generating detectors, and monitoring the occurrence of anomalies. In the defining self phase, the algorithm establishes the normal behavior patterns of a monitored system and defines the patterns as self. In the generating detectors phase, the algorithm generates a number of immature T-cells with random patterns. Any immature T-cells with patterns equal to any self patterns should be discarded. During the monitoring phase, any newly profiled patterns are compared to existing T-cell detector patterns to detect anomalies in the system.

2.5 Clustering Methods

Clustering is one of the unsupervised machine learning techniques used in IDS. Clustering techniques group samples from dataset based on similarities of the samples and decide the outliers as the anomaly. Cluster association and centroid distance techniques are the two most important categories of clustering in Anomaly-based detection.

1) Ant Clustering Algorithm (ACA) is a bio-inspired algorithm based on ant clusters. In a simple model, ants move randomly in space, pick up items, and deposit items based on the local information. The local information is calculated using the characteristic features from each data instances and is used to build the cluster [4].
2) k-means clustering partitions the given dataset into n clusters, and each cluster has a cluster center. Any sample assigned to each cluster has a minimum distance to the centroid of

the cluster. The Euclidean distance can be used to determine the distance between each sample and the centroid [1].

In general, k-means clustering algorithm is very sensitive to the number of initialization clusters, which directly affects the results of clustering. ACA doesn't require a pre-specified number of clusters to initialize, so that ACA can overcome the high sensitivity defect of traditional clustering during initialization, thereby improving the effect of the clustering [2].

3 Our Proposed IDS

Our proposed IDS is illustrated in Figure 1, which consists of two main engines; the clustering engine and the AIS engine from [1]. The clustering engine performs the network traffic clustering into the self or non-self clusters through clustering techniques. The AIS engine consists of agents that cooperate for the intrusion detection.

The AIS engine trains the primary detectors, which are generated by the negative selection algorithm, based on the received information from the clustering engine.

3.1 Clustering Engine

The clustering engine utilizes the ACA method to group the network traffic into clusters. After building clusters of dataset, the clustering engine labels each data instances as self or non-self. The clustering engine passes labeled dataset to the AIS engine, and the AIS engine makes and trains detectors based on the received dataset from the cluster engine.

3.2 AIS Engine

The proposed AIS engine makes detectors by using the negative selection

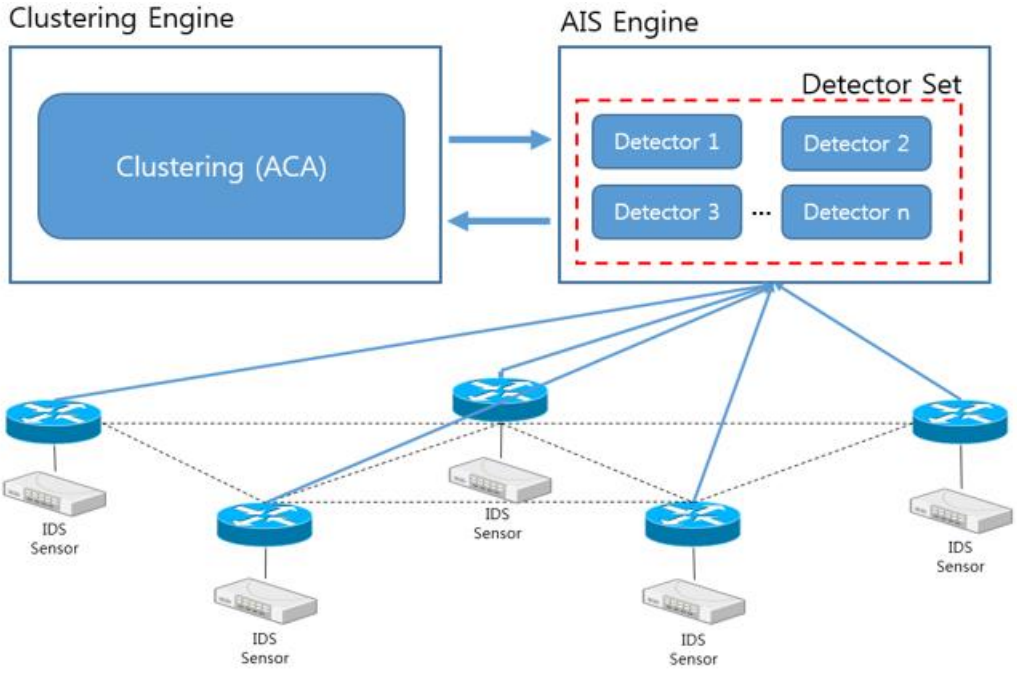

Figure 1 Proposed IDS architecture

algorithm.

The engine converts the network traffic information into the binary string and generates and trains the primary detectors by using the negative selection algorithm.

The negative selection algorithm generates a number of random detectors (immature detectors) and trains the detectors with samples of labeled traffic from the cluster engine. If the pattern of each immature detector matches the pattern of each self sample of the dataset, then the system will discard the detector and generate another detector. After checking all immature detectors with all self samples, the remaining detector sets undergo the next step of the negative selection algorithm and become mature detectors. Each mature detector will be checked with all non-self samples of labeled traffic from cluster engine, and only detectors which match with any non-self sample will be added to detector set. This process will continue until all non-self traffics are matched with at least three mature detectors.

After the detector generation phase is finished, detectors of the detector set monitor network traffic to detect abnormal traffic.

4 Comparison

Farhoud, *et al.* [1] proposed similar IDS architecture to our design. They proposed combining AIS and Density-Based Spatial Clustering of Applications with Noise (DBSCAN) which is one of the clustering algorithm methods to detect unknown-attacks. Also they compared the performance of their IDS with combining AIS and k-means clustering method.

Because the basic architecture is similar, the clustering algorithm is important difference. The comparison of important features between three IDS is summarized in Table 2.

k-means clustering needs the minimum number of parameters and has robustness to data density. However, k-means clustering has highly sensitivity of initialization and data dimension. Combining AIS and k-means clustering method represents 43.1% of DR and 15.6% of FPR. DBSCAN needs two parameters and has robustness to initialization. But DBSCAN suffered from sensitivity of data density and data dimension. Combining AIS and DBSCAN method represents 58.9% of DR and 0.8% of FPR. ACA needs the maximum number of parameters. But ACA is strong to high density and high dimensional data. The algorithm is insensitive to initialization. Real network traffic has high density and dimensional. Thus, our proposed IDS; combining AIS and ACA can be the best solution for clustering in IDS.

5 Concluding Remarks

5.1 Summary

In this paper, a novel architecture for an IDS to detect unknown-attacks was presented. Combining ACA and AIS, our IDS is composed of two parts: the cluster engine and the AIS engine. In the cluster engine, ACA builds clusters based on dataset and labels self or non-self to each data instances. The AIS Engine makes and trains detectors by using labeled dataset

Table 2 Comparison of features

	AIS + k-means [1]	AIS + DBSCAN [1]	Our proposed IDS
# of parameters	1	2	4 [2]
Insensitivity of initialization	X	O	O [2]
Insensitivity of data density	O	X	O [9]
Insensitivity of data dimension	X	X	O [9]
DR (%)	43.1	58.9	65*
FPR (%)	15.6	0.8	3*

O : insensitive

X : sensitive

* : estimate

from the cluster engine. The negative selection algorithm is used in this phase. Compared to other methods such as combining AIS and k-means, our design presents better characteristics and performance.

5.2 Future work

As future work, we should implement the proposed IDS and conduct a detailed analysis.

This research is based on KDD Cup 99 Dataset which is too old to represent the current network environment. Thus, the use of more recent dataset is important for a realistic performance evaluation. UNB ISCX Dataset [10] can be a considerable candidate.

Acknowledgement

This work was partly supported by the ICT R&D program of MSIP/IITP, Republic of Korea. [1391104001, Research on Communication Technology using Bio-inspired Algorithm] and the KUSTAR-KAIST Institute, under the R&D program supervised by the Korea Advanced Institute of Science and Technology (KAIST), South Korea.

References

[1] Farhoud Hosseinpour, Payam Vahdani Amoli, Fahimeh Farahnakian, Juha Plosila, and Timo Hämäläinen, “Artificial Immune System Based Intrusion Detection: Innate Immunity using an Unsupervised Learning Approach”, International Journal of Digital Content Technology & its Applications 8.5, 2014.

[2] Tao Li and Nan-feng Xiao, “Novel heuristic dual-ant clustering algorithm for network intrusion outliers detection”, Optik-International Journal for Light and Electron Optics 126.4, 2015, 494-497.

[3] Leandro Nunes de Castro and

Jonathan Timmis, “Artificial Immune Systems: A New Computational Approach”, Springer Verlag, London, UK., 2002.
[4] Urszula Boryczka, “Ant clustering algorithm”, Intelligent Information Systems, 1998, 455-458.
[5] Karen Scarfone and Peter Mell, “Guide to intrusion detection and prevention systems”, NIST Special Publication 800, 2007.
[6] Sevil Şen, John Clark, and Juan Tapiador, “Power-aware intrusion detection in mobile ad hoc networks”, Ad hoc networks, Springer Berilin Heidelberg, 2010, 224-239.
[7] Salvatore Stolfo, Wenke Lee, and Andreas Prodromidis, “Cost-based modeling for fraud and intrusion detection: Results from the JAM project”, DARPA Information Survivability Conference and Exposition, DISCEX’00. Proceedings Vol. 2, IEEE, 2000.
[8] Stephanie Forrest and Catherine Beauchemin, “Computer Immunology” Communications of the ACM, vol. 40, no. 10, 1997, 88-96.
[9] Julia Handl, Joshua Knowles, and Marco Dorigo, “Ant-based clustering: a comparative study of its relative performance with respect to k-means, average link and 1D-SOM”, Proceedings of the Third International Conference on Hybrid Intelligent Systems, IOS Press, 2003.
[10] Ali Shiravi, Hadi Shiravi, Mahbod Tavallaee, and Ali Ghorbani, “Toward developing a systematic approach to generate benchmark datasets for intrusion detection”, Computers & Security, Vol.31.3, 2012, 357-374.