SCIS 2016 2016 Symposium on
Cryptography and Information Security
Kumamoto, Japan, Jan. 19 - 22, 2016
The Institute of Electronics,
Information and Communication Engineers

Another Fuzzy Anomaly Detection System Based on Ant Clustering Algorithm

Muhamad Erza Aminanto* HakJu Kim* Kyung-min Kim* Kwangjo Kim*

Abstract: Attacks against computer networks are evolving rapidly. Conventional intrusion detection system based on pattern matching and static signatures have a significant limitation since the signature database should be updated frequently. The unsupervised learning algorithm can overcome this limitation. Ant Clustering Algorithm (ACA) is a popular unsupervised learning algorithm to classify data into different categories. However, ACA needs to be complemented with other algorithms for the classification process. In this paper, we present a fuzzy anomaly detection system that works in two phases. In the first phase, the training phase, we propose ACA to determine clusters. In the second phase, the classification phase, we exploit a fuzzy approach by the combination of two distance-based methods to detect anomalies in new monitored data. We validate our hybrid approach using the KDD Cup'99 dataset. The results indicate that, compared to several traditional and new techniques, the proposed hybrid approach achieves higher detection rates and lower false alarm rate.

Keywords: Unknown attacks, unsupervised learning, ant clustering algorithm, fuzzy logic.

1 Introduction

In recent years, various schemes have been proposed for computer network protection from malicious party. Intrusion Detection System (IDS) has emerged as one of the most common parts for every network security infrastructures [1]. IDS is usually classified into misuse detection and anomaly detection [2]. Misuse detection techniques usually utilize signature-based approach to detect attacks. The approach is intended to identify known attack patterns. Although misused detection techniques are most commonly used in practice [2], these techniques have a significant drawback [3]. The main drawback of misuse detection is incapability to detect unknown attacks since it considers known signature of attacks. In order to maintain the performance of misuse detection, we need to keep signature of attacks updated every time which is burdensome. In addition, attackers usually combine previous attacks, so called polymorph attacks [3]. This kind of attack is more difficult to develop appropriate signatures for misuse detection. There are two possible ways, the first one, generate several signatures that cover all possible variation of attacks. Another one, generalize the signatures which means higher false alarm [3]. On the other hand, anomaly detection focuses on detecting unusual activity patterns in the observed data [2]. Anomaly detection approach usually deals with statistical analysis and data mining problems [4], which are able to detect novel attacks without prior knowledge since the classification model has the generalization ability to extract intrusion pattern and knowledge during the training phase[4].

It is difficult and costful to obtain bulk of labeled network connection records for supervised training. The clustering analysis has emerged as an anomaly intrusion detection approach in recent years [4]. Clustering is an unsupervised data exploratory technique that partitions a set of unlabeled data patterns into groups or clusters such that patterns within a cluster are similar to each other but dissimilar to other clusters' pattern [4]. Ant Clustering Algorithm (ACA) is one of the most widely used clustering approaches which is originated from swarm intelligence. ACA is an unsupervised learning algorithm that is able to find near-optimal clustering solution without predefined number of clusters needed [4]. However, ACA is rarely used in intrusion detection as the exclusive method for classification. Instead, ACA is combined with other supervised algorithms such as Self Organizing Maps (SOM) and Support Vector Machine (SVM) in order to provide better classification result [1]. Based on Karami *et al.*[5] experiments, fuzzy logic approach can be used to improve classification result.

In this paper, we propose a novel hybrid IDS scheme based on ACA and fuzzy logic approach. Our proposed scheme comprises two phases, training and classification. We apply ACA for training phase and fuzzy logic approach for classification phase. We choose fuzzy approach as classification phase, because fuzzy approach can reduce the false alarm rate with higher reliability in determining intrusion activities [5]. The experimental results on the KDD Cup'99 dataset demonstrate that our scheme can provide accurate and robust clustering and classification solution with high detection rate and

* School of Computing, Korea Advanced Institute of Science and Technology (KAIST), 291 Gwahak-ro, Yuseong-gu, Daejeon, 34141, Korea. {*aminanto*, *ndemian*, *saza*1234, *kkj*}@kaist.ac.kr.

low false alarm rate. Our contribution in this paper is two-fold. First, we examine the hybrid IDS approach published by Karami *et al.* [5] with different clustering algorithms. We employ ACA instead of Particle Swarm Optimization (PSO) and K-means algorithm. Second, we adopt Karami's fuzzy rule [5] with different fuzzy membership functions.

This paper is organized as follows: Section 2 provides previous publications which inspire us to work on this problem. Section 3 explains the background of this paper such as IDS, ACA, Fuzzy logic and KDD Cup'99. Section 4 describes our proposed method. Section 5 contains experimental results and analysis. Finally we conclude in Section 6.

2 Related Work

There are many different IDS schemes that use hybrid approaches to integrate the ant-based clustering model with other machine learning and soft computing algorithms [4]. They include the cellular automata [6], K-means algorithm [7], self-organizing map [8], fuzzy C-mean algorithm [9] and fuzzy if-then rule system [10]. Those schemes except Abadeh *et al.* [10], are different from our proposed scheme since they are not using fuzzy if-then rule system. Meanwhile, our proposed scheme differs from Abadeh *et al.* [10] by the goal of the IDS, which their intention is to aim misused detection while we aim anomaly detection.

One of the most recent hybrid IDS was proposed by Karami *et al.* [5] at 2014. Unlike Karami's [5] work which focuses on Content-Centric Networks, we aim ordinary networks. They proposed a hybrid IDS system using PSO-K-means algorithm and fuzzy approach. Basically, their scheme contains two phases, training and classification. They applied a novel combination of PSO and K-means algorithm for training phase in order to provide better clustering result. However, according to Kolias *et al.* [1], ACA-based IDS provides higher detection rate than other IDS schemes, including PSO and K-means algorithm. Thus, in this paper, we investigate the effectiveness of using ACA instead of PSO and K-means algorithm as a clustering method. For the classification phase, Karami *et al.* [5] utilized fuzzy if-then rules to give a fuzzy detection of normal and abnormal results in the new monitoring data set that does not appear in the training set. They claimed that by using fuzzy rules, false alarm rate can be reduced.

3 Preliminaries

In this section we describe general overview of related terms such as IDS, ACA, fuzzy logic approach, and KDD Cup'99 Dataset.

3.1 IDS

According to the guidance from National Institute of Standards and Technology (NIST) [11], intrusion detection is defined as "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices". IDS is a system that is designed to perform all the procedures relevant to intrusion detection [1]. There are many varieties of techniques and frameworks that are implemented in IDS. In general, IDSs are comprised of:

- A set of sensors that collects both malicious and normal data from the monitored system [1]. Sensors may be part of the system or external devices depends on the type of IDS.
- An analyzer engine that collects all data from sensors and analyses them. The engine usually located in central point. The engine has capability to reconfigure the protected system properly if the results of the analysis indicate an intrusion occurred. [1].
- A report system that alerts the responsible party when suspicious events occurred [1].

The IDS based on misuse detection contains signatures of known attacks. The list of signatures is utilized by the analyzer engine during the data analysis step and must be frequently updated to include the signatures of the latest attacks. In addition, several IDSs might have response engine [1]. The response engine might be able to take actions automatically or manually by the command of the administrator.

There are many different classifications of the existing IDS based on different criteria. One distinction can be made in terms of the location of the active sensing components of the IDS. Based on this attribute, the IDS can be classified into host-based and network-based [1]. In host-based approaches the sensor components are installed on each host that requires protection. Meanwhile, a network-based IDS monitors the network that contains the hosts of interest. This type of IDS is usually installed on multiple dedicated machines, which are possibly different from the protected hosts, and monitors the network traffic.

Other categorization is based on the adopted data analysis approach. In this case, IDS may fall into one of the two main groups: misuse detection and anomaly detection [1]. The first approach examines the activity of the entire infrastructure for patterns of misuses known beforehand, usually referred to as attack identities. On the other hand, anomaly detection approaches analyze the behavior of the protected system over time toward extracting an approximate estimation of what behavior is considered normal or legitimate. Any action that significantly deviates from that kind of behavior is considered an attack.

In general, an IDS must be able to identify intrusions with high accuracy. At the same time, an IDS should be able to distinguish between legitimate and intrusive actions. These two criteria have been associated

with two performance evaluation variables: Detection Rate (DR) and False Alarm Rate (FAR). Kolias *et al.* [1] defined DR as the ratio of the number of correctly detected attacks to the total number of attacks. Meanwhile FPR, also known as false positive rate, defined as the ratio of the number of normal connections that are classified incorrectly as attacks to the total number of normal connections [1]. An IDS usually tries to maintain high detection rates and keep false alarm rates as low as possible in the same time.

3.2 ACA

ACA simulates ant random walks on a two-dimensional grid which is all data objects are spread randomly [12]. Unlike the dimension of the input data, each data instance is randomly projected onto a cell of the grid. A grid cell can indicates the relative position of the data instance in the two-dimensional grid. The general idea of ACA is to keep similar items in their original N-dimensional space. Vizine *et al.* [12] assumed that each site or cell on the grid can be resided by at most one object, and one of the two following situations may occur: (i) one ant holds an object i and evaluates the probability of dropping it in its current position; (ii) an unloaded ant evaluates the probability of picking up an object. An ant is selected randomly and can either pick up or drop an object at its current location [12].

The probability of picking up an object increases by disparity among objects in the surrounding area and *vice versa*. In contrast, the probability of dropping an object increases by high similarity among objects in the surrounding area. Vizine *et al.* [12] defined *d(i,j)* in Eq. (1) as the Euclidean distance between objects i and j in their N-dimensional space. The density distribution function for object i, at a particular grid location, is defined by Eq. (1) as follows:

$$f(i) = \begin{cases} \frac{1}{s^2}\sum_j (1 - d(i,j)/\alpha) & f(i) > 0 \\ 0 & Otherwise, \end{cases} \quad (1)$$

where s^2 is the number of cells in the surrounding area of i and α is a constant that depicts the disparity among objects. The *f(i)* might reach maximum value when all the sites in the surrounding area are occupied by similar or even equal objects. The probability of picking up and dropping an object i is given by Eqs. (2) and (3), respectively:

$$P_{pick}(i) = (\frac{k_p}{k_p + f(i)})^2, \quad (2)$$

$$P_{drop}(i) = \begin{cases} 2f(i) & f(i) < k_d \\ 1 & Otherwise, \end{cases} \quad (3)$$

where the parameters k_p and k_d are threshold constants of the probability of picking up and dropping an object, respectively. A loaded ant considers the first empty cell in its local area to drop the object. Meanwhile, the current position the object can be already occupied by another object[12].

Tsang *et al.* [4] define two variables: intra-cluster and inter-cluster distance in order to measure ACA performance. High intra-cluster distance means better compactness. Meanwhile, high inter-cluster distance means better separateness. A good ACA should provides minimum intra-cluster distance and maximum inter-cluster distance in order to presents the inherent structures and knowledge from data patterns.

3.3 Fuzzy Approach

Fuzzy approach is a method of representing the ambiguity and imprecision of a logic that usually only 1 and 0 in digital form. This property of fuzzy set is appropriate to be exploited as anomaly detector for two main reasons [13]:

1. The anomaly detection problem usually includes several numeric attributes in collected data and various derived statistical measurements. Constructing models on numeric data directly might cause many errors in detection.

2. The security term itself involves fuzziness, because the boundary between normal and abnormal is not well defined [5].

Fuzzy logic usually used together with other popular data mining techniques in order to detect outlier. Malicious behavior is naturally different from normal behavior, then abnormal behavior might be considered as outlier. Fuzzy logic can help to construct more abstract and flexible pattern for intrusion detection and thus greatly increase the robustness adaption ability of detection system [5]. Therefore, fuzzy approach can reduce the FAR with higher reliability in determining intrusive activities, as any data instance whether normal or attack, might be similar to some clusters. The distance to clusters represents similarity, the nearer the distance means that the data instance is similar to that cluster.

3.4 KDD Cup'99 Dataset

KDD Cup'99 dataset has been the most widely used dataset for the evaluation of anomaly detection methods [14]. The dataset is based on the data captured in DARPA'98 IDS evaluation program. KDD Cup'99 dataset consists approximately 4,900,0000 single connection instance. Table 1 shows the packet distribution of KDD Cup 99 dataset [15]. Each instance contains 41 features and is labeled as either normal or attack instance. The dataset provides four distinct attack types as follows:

1. **Probing Attack**: an attacker attempts to collect information about computer networks in the purpose of bypassing the security controls. An example of probing attack is port scanning.

2. **Denial of Service (DoS) Attack**: an attack in which the attacker prevents legitimate users from accessing authorized data. The attacker made

Table 1: Packet Distribution of KDD Cup'99 Dataset

Type	# of Packets	Proportion (%)
Normal	972,781	19.86
Probe	41,102	0.84
DoS	3,883,370	79.28
U2R	52	0.00
R2L	1,126	0.02
Total	4,898,431	100

computing resources too exhausted to handle legitimate requests by flooding the network with unnecessary packet requests. An example of DoS attack is syn flood attack.

3. **User to Root (U2R) Attack**: an attacker starts the attack with accessing to a normal user account on the system. Then, the attacker exploit the vulnerability to gain root access to the system. An example of U2R attack is *xterm* exploitation.

4. **Remote to Local (R2L) Attack**: This kind of attack occurred by an attacker who has the ability to send packets to a machine over a network but does not have an account on that machine. The attacker exploits some vulnerabilities to gain local access as a user of that machine remotely. An example of R2L attack is *ftp_write* exploitation.

4 Our Approach

This section describes the details of our approach. Basically, our approach consists of two main phases, training and classification. Similar to other approaches, our scheme is illustrated in Fig. 1. Each phase is also described as follows:

4.1 Training Phase

The training phase implements ACA in order to clusters the network traffic. ACA incorporates several initialization steps. Thus, it needs several input parameters such as the size of grid area, the number of ants, the size of local area, and threshold constant. After the clustering phase finished, we label each data instances according to the cluster result [15]. The training phase passes these labeled dataset to the Fuzzy Inference System (FIS) in the classification phase.

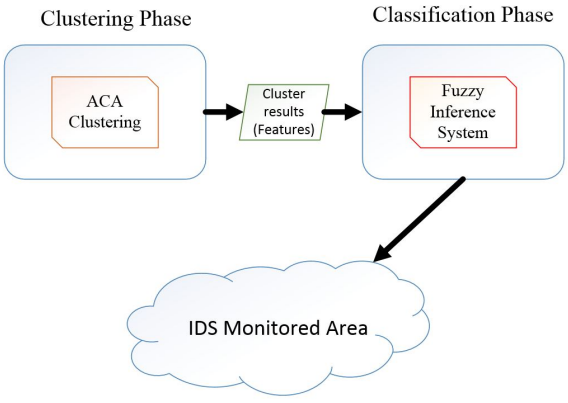

Figure 1: Two Phases of our scheme

4.2 Classification Phase

The labeled dataset from the training phase are sent to the second phase for anomaly detection when new data arrive. In the classification phase, a fuzzy decision approach is applied to detect attacks. We calculate Euclidean distance of each test data to all clusters as an input to the FIS. Eq. (4) shows the Euclidean distance of two points x and y, where x_i and y_i represent features of each test data instance and training data instance within cluster, respectively. In this case, N represents total features in KDD Cup'99 dataset [16] which has 41 features on each data instances.

$$Distance(x, y) = \sqrt{\sum_{i=1}^{N}(x_i - y_i)^2}. \quad (4)$$

We deploy a combination of two distance-based [5] methods, *i.e.*, nearest to normal and abnormal:

1. **Nearest to Normal**: The distance between a test data instance and each cluster is calculated using average linkage of Euclidean distance. Average linkage approach considers small variances [5], because the approach considers all members in the cluster rather than just a single member. In addition, the average linkage approach tends to be less influenced by the extreme values than other distance methods [17]. A test data instances is classified as nearest to normal when it has minimum average Euclidean distance among clusters labeled as normal cluster and *vice versa*. This distance-based classification allows us to detect whether normal or abnormal traffic by comparing features similarity that listed in the training data set.

2. **Nearest to Abnormal**: Similar as before, we also calculate average linkage of Euclidean distance in order to find the minimum distance to abnormal cluster. A test data instance is classified as nearest to abnormal when the data instance has minimum average Euclidean distance among clusters labeled as abnormal cluster and *vice versa*.

The proposed fuzzy detection method consists of two inputs (nearest to normal and abnormal), one output, and four main parts: fuzzification, rules, inference engine, and defuzzification [5]. In fuzzification step, a crisp set of input data is converted to a fuzzy set using fuzzy linguistic terms and membership functions. Next, we construct rule base. Afterwards, an inference

is made and combined based on the set of rules. In defuzzification step, the results of fuzzy inference are mapped to a crisp (non-fuzzy) output using the output membership functions. Finally, if the crisp output is bigger than a predefined threshold, a test data instance is considered as an abnormal instance, otherwise it is a normal instance.

5 Evaluation

5.1 Performance Measurement

In order to evaluate the performance of our proposed approach, we use DR, FAR and False Negative Rate (FNR). We calculate DR by number of attack instances detected as attacks divided by total of attack instances included in test dataset. We have 393 data of attack instances. FAR, also known as false positive rate, is legitimate packet detected as a malicious packet. FAR calculated by number of legitimate instances detected as attack instances divided by total normal (legitimate) instances included in the data test. We are incorporating 19,268 legitimate instances. Lastly, FNR represents number of attacks that unable to be detected by our proposed approach. The FNR value can be calculated by one minus DR.

5.2 Experiment Setup

In order to validate our approach, we use experiment scheme as shown in Fig. 2. We need to customize the KDD Cup'99 dataset in order to get appropriate traffic data that reflects real network traffic. Also, we need to prepare two sets of data: training and test dataset. Table 2 shows the training dataset that we used as an input to ACA in clustering phase as shown in Fig. 2. As mentioned in Sec.4.1, ACA needs several input parameters, we define the parameter as follows:

- Size of grid area: 600 X 600 size of 2D plane,
- Number of ants: 1000 ants,
- size of local area: 3 X 3 local area,
- Threshold constant: 15.

ACA provides clusters that consolidates similar feature data instances. We label big and small size clusters as normal and attack clusters, respectively. We prepare the test dataset as shown in Table 3. The dataset is passed to pre-processing phase as depicted in Fig. 2. In this phase, we measure the Euclidean distance between each data instance in the test dataset and all data instances in the training dataset. Then, we define two values: closest to normal and abnormal, as an input parameter to the Fuzzy Inference System (FIS).

5.3 Classification Phase

We use MATLAB fuzzy logic toolbox for FIS-based intrusion detection. The classification phase is structured by following components:

1. Two fuzzy sets of input variables: nearest to normal and abnormal; nearest to normal membership are: Very Close, Close, Average, Far, Very Far; nearest to abnormal membership are: Far, Average, Close.
2. A fuzzy set of output variable: Alarm; alarm membership function: Normal, Less Prone, High Prone, Abnormal.
3. Fuzzy Membership functions: Figs. 3,4, and 5 show fuzzy membership function, for nearest to normal, abnormal and alarm, respectively.
4. Fuzzy rules: Table 4 shows complete fuzzy rules while Table 5 shows more detailed fuzzy rules.
5. Inference: We use Mamdani fuzzy inference by fuzzy set operation as max and min for OR and AND, respectively [5]. Figs. 6 and 7 show a sample solution area from fuzzy inference and in 3D form, respectively.
6. Defuzzifier: We use Center of Gravity algorithm as shown by Eq.(5).

$$CenterOfGravity = \frac{\int_{min}^{max} u * \mu(u)d(u)}{\int_{min}^{max} \mu(u)d(u)}, \qquad (5)$$

where u represents the output variable, μ denotes the membership function after accumulation, and min and max are lower and upper limits for defuzzification, respectively.

5.4 Experiment Result

This section shows our experimental results. Recall in the defuzzification step, the results of fuzzy inference

Table 2: Our Training Dataset

Type	# of Packets	Proportion (%)
Normal	78,101	98.00
Probe	398	0.50
DoS	761	0.96
U2R	35	0.04
R2L	398	0.50
Total	79,602	100

Table 3: Our Test Dataset

Type	# of Packets	Proportion (%)
Normal	19,268	98.00
Probe	98	0.50
DoS	277	1.41
U2R	17	0.09
R2L	1	0.00
Total	19,661	100

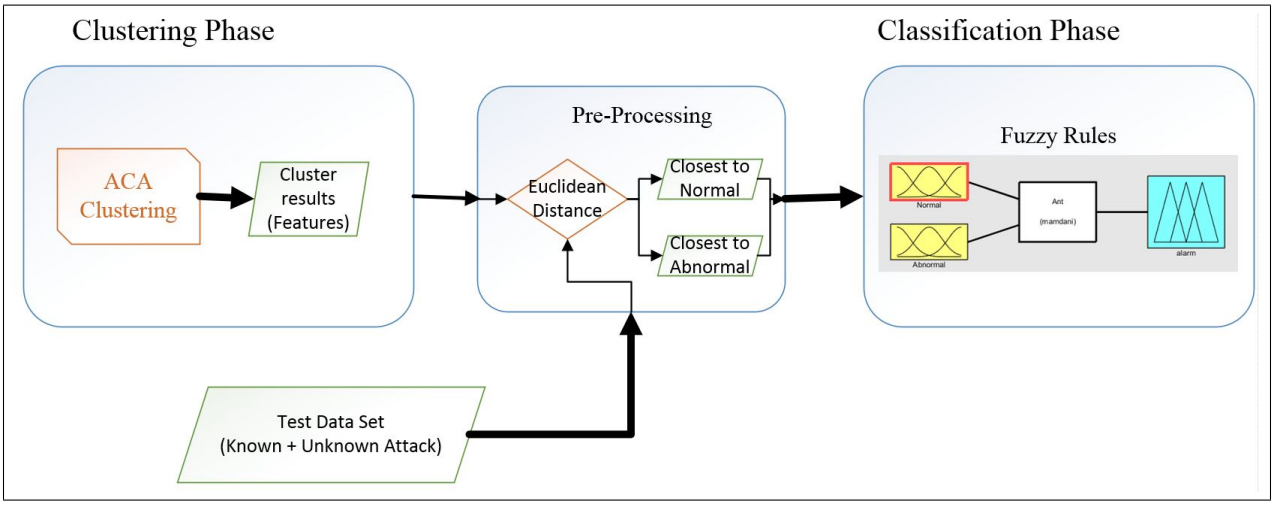

Figure 2: Experimental Scheme

Table 4: Fuzzy Rules

Nearest to Abnormal	**Nearest to Normal**				
	VeryClose	Close	Average	Far	VeryFar
Close	HighProne	HighProne	Abnormal	Abnormal	Abnormal
Average	LowProne	LowProne	HighProne	HighProne	HighProne
Far	Normal	Normal	Normal	HighProne	HighProne

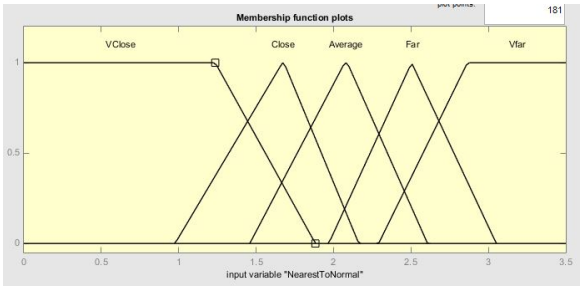

Figure 3: Membership Function for Normal Input

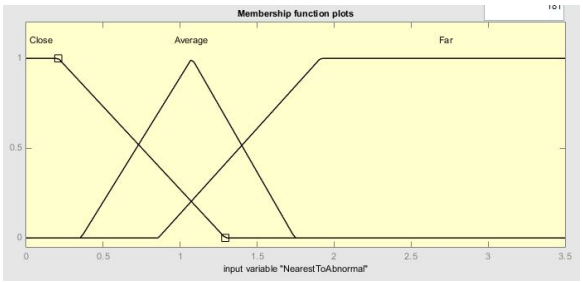

Figure 4: Membership Function for Abnormal Input

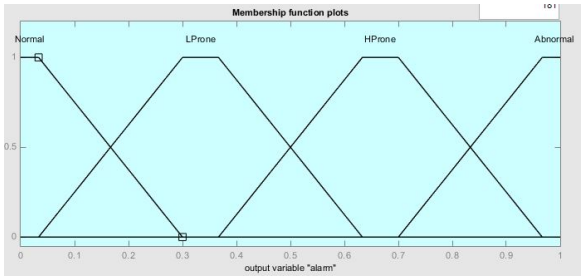

Figure 5: Membership Function for Alarm Output

are mapped to a crisp (non-fuzzy) output using the output membership functions. If the crisp output is bigger than a predefined threshold (from now on called fuzzy threshold), a test data instance is considered as an abnormal instance, otherwise it is a normal instance. Table 6 shows the performance of our approach using different fuzzy thresholds. We can see that the bigger the fuzzy threshold, the bigger the detection rate (DR). Unfortunately, we also have bigger FAR as a trade-off. We note that 0.65 as fuzzy threshold provide best performance among others with DR = 92.11% and FAR = 10.03%. It means that there are 1,936 legitimate instances detected as an attack. Also, 31 out of 393 attack data instances aren't detected as attacks. Thus, we conclude that 0.65 is the optimal value for the fuzzy threshold.

In order to provide the proper measurement, we compare our scheme with other similar schemes as mentioned by Farhoud *et al.* [18]. They proposed a hybrid

Table 5: Some Fuzzy Rules in Proposed System

IF Normal=*Average* and Abnormal=*Far* **THEN** Alarm=*Normal*
IF Normal=*Close* and Abnormal=*Average* **THEN** Alarm=*LowProne*
IF Normal=*Far* and Abnormal=*Average* **THEN** Alarm=*HighProne*
IF Normal=*VeryFar* and Abnormal=*Close* **THEN** Alarm=*Abnormal*

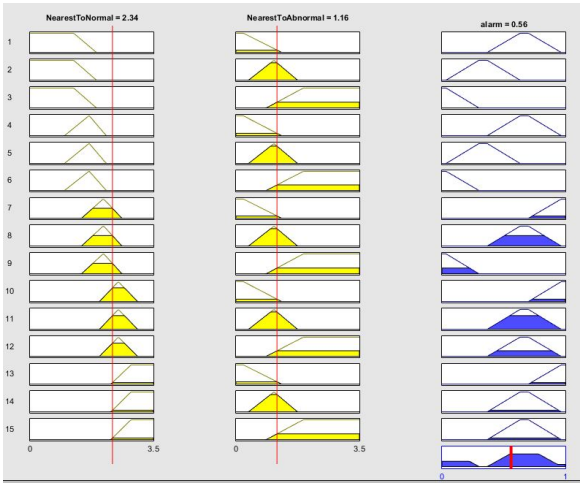

Figure 6: Sample of Fuzzy Inference

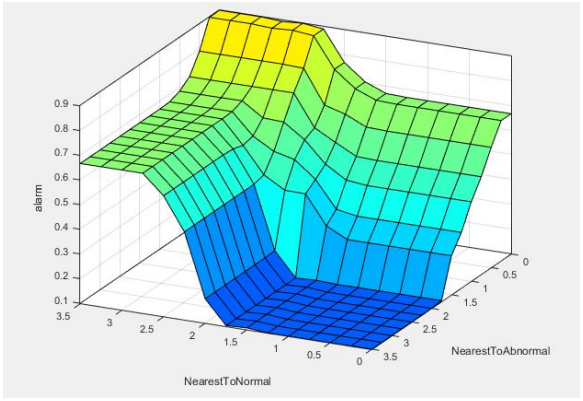

Figure 7: 3D Rule View

Table 6: Performance of Our Proposed Scheme

Fuzzy Threshold	FAR (%)	DR (%)	FNR (%)
0.70	9.40	0.00	100.00
0.65	10.03	92.11	7.89
0.60	20.81	94.91	5.09
0.55	32.35	94.91	5.09
0.30	97.25	98.73	1.27

Table 7: Results Comparison

Method	DR (%)	FAR (%)
AIS+K-means [18]	43.1	15.6
AIS+DBSCAN [18]	58.9	0.8
Our Proposed Scheme	92.11	10.03

scheme of Artificial Immune System (AIS) and Density Based Spatial Clustering of Applications with noise (DBSCAN). Similar to our approach, their approach exploits two phases: clustering and detection phase. In addition, they also provide the performance result of another IDS scheme based on AIS and K-means clustering. Based on these similarities, we compare the performance of our scheme and the performance of Farhoud's *et al.* [18] schemes. Table 7 shows the comparison of three different schemes.

ACA is a proper algorithm for high density and high dimensional data. Also, ACA is insensitive to initialization step. These properties satisfy the needs of real traffic network, which has high density and high dimensional data. Although ACA needs many input parameters, by combining it with FIS, our proposed scheme is able to achieve significantly higher DR compared to other two schemes. However, our proposed scheme provides quite high FAR which is 10.03%, but the value is still better than that of AIS+K-means scheme. Thus, we can claim that our proposed scheme can provides high detection rate and low false alarm rate. We let our high FAR issue as our future work.

6 Conclusion and Future Work

In this paper, we propose a novel fuzzy anomaly detection system based on Ant Clustering Algorithm (ACA) and Fuzzy Inference System (FIS). The system contains two phases: the training phase implementing ACA to cluster training dataset; and the classification phase incorporating the FIS. We define our FIS with two distance values as nearest to normal and abnormal clusters. Experimental results show that our scheme is very effective to detect both known and unknown attacks. However, our scheme still provides high FAR. Thus, we will further investigate this issue in the near future.

Acknowledgement

This work was partly supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government(MSIP) (B0101- 15-1270, 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), Republic of Korea.

References

[1] C. Kolias, G. Kambourakis, and M. Maragoudakis, "Swarm intelligence in intrusion detection: A survey," *Journal of Computers & Security*, vol. 30, no. 8, pp. 625–642, 2011.

[2] P. Laskov, P. Düssel, C. Schäfer, and K. Rieck, "Learning intrusion detection: supervised or unsupervised?" *Image Analysis and Processing–ICIAP 2005*, pp. 50–57, 2005.

[3] S. Zanero and S. M. Savaresi, "Unsupervised learning techniques for an intrusion detection system," *Proceedings of the 2004 ACM symposium on Applied computing*, pp. 412–419, 2004.

[4] C.-H. Tsang and S. Kwong, "Ant colony clustering and feature extraction for anomaly intrusion detection," *Swarm Intelligence in Data Mining*, pp. 101–123, 2006.

[5] A. Karami and M. Guerrero-Zapata, "A fuzzy anomaly detection system based on hybrid pso-k-means algorithm in content-centric networks," *Journal of Neurocomputing*, vol. 149, pp. 1253–1269, 2015.

[6] P. Albuquerque and A. Dupuis, "A parallel cellular ant colony algorithm for clustering and sorting," *International Conference on Cellular Automata for Research and Industry, ACRI*, pp. 220–230, 2002.

[7] N. Monmarché, M. Slimane, and G. Venturini, "Antclass: discovery of clusters in numeric data by an hybridization of an ant colony with the k-means algorithm," *Internal Report*, no. 213, pp. 1–21, 1999.

[8] T. Mikami and M. Wada, "Data visualization method for growing self-organizing networks with ant clustering algorithm," *Advances in Artificial Life*, pp. 623–626, 2001.

[9] P. M. Kanade and L. O. Hall, "Fuzzy ants as a clustering concept," *Fuzzy Information Processing Society, 2003. NAFIPS 2003. 22nd International Conference of the North American*, pp. 227–232, 2003.

[10] M. S. Abadeh and J. Habibi, "A hybridization of evolutionary fuzzy systems and ant colony optimization for intrusion detection," *The ISC International Journal of Information Security*, vol. 2, no. 1, pp. 33–46, 2010.

[11] K. Scarfone and P. Mell, "Guide to intrusion detection and prevention systems (idps)," *NIST special publication*, vol. 800, no. 94, pp. ES–1, 2007.

[12] A. L. Vizine, L. N. de Castro, and E. Hrusch, "Towards improving clustering ants: an adaptive ant clustering algorithm," *Journal of Informatica*, vol. 29, no. 2, pp. 143–154, 2005.

[13] H. Izakian and W. Pedrycz, "Agreement-based fuzzy c-means for clustering data with blocks of features," *Neurocomputing*, vol. 127, pp. 266–280, 2014.

[14] M. Tavallaee, E. Bagheri, W. Lu, and A.-A. Ghorbani, "A detailed analysis of the kdd cup 99 data set," *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009*, pp. 53–58, 2009.

[15] K. Kim, H. Kim, and K. Kim, "Design of an intrusion detection system for unknown-attacks based on bio-inspired algorithms," *Proceeding of Computer Security Symposium 2015 (CSS 2015)*, 2015.

[16] D. Pelleg and A. W. Moore, "Accelerating exact k-means algorithms with geometric reasoning," *Proceedings of the Fifth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 277–281, 1999.

[17] J. P. Verma, "Cluster analysis: for segmenting the population," *Data Analysis in Management with SPSS Software*, pp. 317–354, 2012.

[18] F. Hosseinpour, V. P. Amoli, F. Frahnakian, J. Plosila, and T. Hämäläinen, "Artificial immune system based intrusion detection: Innate immunity using an unsupervised learning approach," *International Journal of Digital Content Technology and its Applications*, vol. 8, no. 5, pp. 1–12, 2014.