Application of kernel spherical k-means for intrusion detection systems

Zuherman Rustam\textsuperscript{1,a} and Farah Nadhifa\textsuperscript{1,b}

\textsuperscript{1}Department of Mathematics, Faculty of Mathematics and Natural Sciences, Universitas Indonesia, Depok 16424, Indonesia

E-mail: \textsuperscript{a}rustam@ui.ac.id, \textsuperscript{b}farah.nadhifa@sci.ui.ac.id

Abstract. Operational system can be threatened by malicious network activities from intruders or hackers. Consequently, security of a system is indeed become an important subject to tackle this matter. Intrusion Detection System (IDS) is a system which can prevent network traffic and observe suspicious activities in network systems. Therefore, IDS can solve multiple privacy concerns. This paper will propose new method called Kernel Spherical K-Means (KSPKM) that has been modified from Spherical K-Means (SPKM) algorithm by using RBF and polynomial kernel. For our empirical study, we will be using the dataset from KDD Cup 1999 then classified types of attacks into five classes. In the end, we will see which one will produce better results in terms of classification accuracy. We found out that KSPKM succeed to improve clustering accuracy with the highest rate being 98.31% compared to SPKM.

1. Introduction

In recent years, internet user keeps increasing as we mostly need to access information faster due rapid change of information. Therefore, the danger of intruders and hackers also increase as they intend to steal as well as damage the internal systems of our computer that can be achieve through internet connections. For that matter, we need a high-level security system to ensure the safety of our stored information. Intrusion Detection Systems (IDS) have been created to detect any malicious activity or in other words can act as an ‘alarm system’ to prevent stolen or leaked information before Intrusion Prevention System (IPS) take actions. In this research, due to a large amount of data required for IDS we chose to perform machine learning as it can learn and find patterns in data input with short amount of time [1]. From the previous study, machine learning has been applied for IDS by Z. Rustam and A. S. Talita [2] using Fuzzy Kernel C-Means, Z. Rustam and D. Zahras [3] using SVM and Fuzzy C-Means, S. T. Ikram and A. K. Cherukuri [4] using multi class SVM and chi-square feature selection, and Z. Rustam using Fuzzy Support Vector Machines [5]. Therefore, according to these recent studies, we can see that machine learning is a promising technique for IDS.

In this research, we will propose a new machine learning method that has been modified from Spherical K-Means (SPKM) [6] using kernel function called Kernel Spherical K-Means (KSPKM). The aim for adding kernel to the original SPKM is to make K-Means be able to separate non-linear data. We will be using two kinds of kernel which are polynomial and Gaussian radial basis (RBF) kernel. Moreover, we chose to modified SPKM because it is easy to be understood and implemented but occasionally lacks in clustering accuracy [7]. In short, our main objective in this paper is to significantly improve the clustering quality for K-Means, yet to retain its efficiency. In this paper, we will be using KDD 1999 dataset [8] to test out our algorithms so we know how much Kernel Spherical
K-Means fit to be an intrusion detector by observing its clustering accuracy and how long the running time took.

In the next section, we will present a brief explanation about theoretical background of this research. After that, section 3 will give an explanation about the design of our experiments. Then, experimental results will be discussed in section 4. Lastly, we will conclude our research and give future work suggestions in section 5.

2. Theoretical background

2.1. Intrusion detection systems (IDS)
IDS was first introduced by James Anderson in 1980 [8] to identify any intrusion attempt such as breaking into information system or executing actions that are not legally allowed [9]. There are two methods to detect intrusions which are misuse and anomaly detection. The basic idea of misuse detection is it will detect and prevent attacks by learning pattern of attacks. Then if the incoming flow matches the pattern, it will be flagged as malicious. On the other hand, in anomaly detection or as we also known as behavior based method, will determine or set up a normal activity profile of a system so that the rest of system states will be flagged as intrusion attempt [10].

IDSs can also be classified into two categories according to where they look for intrusion that are a host-based IDS (HIDS) and network based IDS (NIDS). HIDS run on individual hosts or devices on the network and will monitor the inbound as well as outbound packets from the device only. It will also alert the administrator if they detect malicious activity on the system. While NIDS will analyzes network traffic at all layers of Open System Interconnection (OSI) model and decide the purpose of traffic occurs. The advantage of NIDS is that they can diagnose traffic from numerous systems at once and are easy to distribute [11].

IDS can determine several types of attack but in this research, we will use four categorized of attacks according to KDD99 [8] dataset named denial-of-service (DoS), probing attacks (Probe), user to root attack (U2R), and remote to local (R2L).

2.2. Kernel Spherical K-Means (KSPKM)
KSPKM is an adjustment of Spherical K-Means (SPKM) which is one form of clustering that can be used to clustered a high-dimensional data. Spherical K-Means algorithm was founded by Shi Zhong [6]. This algorithm is K-Means algorithm with cosine similarity which is a superior measure to Euclidean distance. This algorithm tends to maximize the objective function [6]:

\[ L = \sum_x x^T \mu_{k(x)} \]  

where:
- \( k(x) = \text{argmax}_k x^T \mu_k \)
- \( x^T \) = data in vector form.
- \( \mu_k \) = centroid vector (mean vector) at \( k \) cluster

The main difference from Standard K-Means is that the re-estimated mean vector \( \{ \mu \} \) need to be normalized to unit-length. Therefore, the first step will be initialization which will be defining the proportion of data training used and the amount of class that is \( K = 5 \) because the data consist 5 different classes for each feature. We will get into the detail and explanation of each class and feature in Section 3. Figure 1 will show the SPKM algorithm that we use in this research [6].
K-Means use Norm Euclidean (2) for measuring distance between \( x \) and \( \mu \) [6]:

\[
d(x, \mu) = \|\mu\|^2 + \|x\|^2 - 2x^T \mu
\]  

Furthermore, we will modify SPKM by mapping data from the original space to another higher space using kernel function defined as \( K(x_i, \mu_k) = \phi(x_i) \cdot \phi(\mu_k) \). The idea in this modification is that to alter the inner product \( x^T \cdot \mu \) from the previous objective function (1) with \( K(x_i, \mu_k) \). Then, it will be resulting to a new equation such as KSPKM objective function (3) and distance function (4) as follows

\[
L = \sum_{i} K(x_i, \mu_k)
\]

\[
d(x, \mu_k) = \|K(x_i, \mu_k)\|^2 + \|x\|^2 - 2x^T K(x_i, \mu_k)
\]

with \( y_n = \arg \max_k K(x_i, \mu_k) \). Thereafter, choosing two kind of kernel functions to be compared that are Gaussian radial basis function (RBF) kernel (5) and polynomial kernel (6) with the formulation as follows:

\[
K(x_i, \mu_k) = \exp \left( -\frac{\|x_i - \mu_k\|^2}{2\sigma^2} \right)
\]

\[
K(x_i, \mu_k) = (x_i \cdot \mu_k + 1)^d
\]

so that the algorithm in Figure 1 will be modified into the following algorithm which shown in Figure 2 below.

\[
\]

The idea in this modification is that to alter the inner product \( x^T \cdot \mu \) from the previous objective function (1) with \( K(x_i, \mu_k) \). Then, it will be resulting to a new equation such as KSPKM objective function (3) and distance function (4) as follows

\[
L = \sum_{i} K(x_i, \mu_k)
\]

\[
d(x, \mu_k) = \|K(x_i, \mu_k)\|^2 + \|x\|^2 - 2x^T K(x_i, \mu_k)
\]

with \( y_n = \arg \max_k K(x_i, \mu_k) \). Thereafter, choosing two kind of kernel functions to be compared that are Gaussian radial basis function (RBF) kernel (5) and polynomial kernel (6) with the formulation as follows:

\[
K(x_i, \mu_k) = \exp \left( -\frac{\|x_i - \mu_k\|^2}{2\sigma^2} \right)
\]

\[
K(x_i, \mu_k) = (x_i \cdot \mu_k + 1)^d
\]

so that the algorithm in Figure 1 will be modified into the following algorithm which shown in Figure 2 below.

\[
\]
Figure 2. KSPKM algorithm.

Adding kernel function to original SPKM could make the data linearly separable, since K-Means clustering can only separate non-convex data. By that, we aim to obtain a better clustering method for detecting intrusion.

3. Experimental designs

3.1. Dataset and features

We will test the constructed algorithms using dataset from KDD99 [8] that contains more than 500,000 data with 24 different types of attacks which has been categorized into four group that are DoS, Probe, R2L, and U2R.

Each data will have total of 41 features as a variable predictor that has been labelled into normal and attacks. All 41 features are listed in Table 1 below.

Table 1. Features for each data

| No  | Feature                  | No  | Feature                  | No  | Feature                  |
|-----|--------------------------|-----|--------------------------|-----|--------------------------|
| 1   | duration                 | 15  | su_attempted             | 29  | same_srv_rate            |
| 2   | protocol_type            | 16  | num_root                 | 30  | diff_srv_rate            |
| 3   | service                  | 17  | nu_file_creations        | 31  | srv_diff_host_rate       |
| 4   | flag                     | 18  | num_shells               | 32  | dst_host_count           |
| 5   | src_bytes                | 19  | num_access_file          | 33  | dst_host_srv_count       |
| 6   | dst_bytes                | 20  | num_outbound_cmds        | 34  | dst_host_same_srv_rate   |
| 7   | land                     | 21  | is_host_login            | 35  | dst_host_diff_srv_rate   |
| 8   | wrong_fragment           | 22  | is_guest_login           | 36  | dst_host_same_src_port_rate |
| 9   | urgent                   | 23  | count                    | 37  | dst_host_srv_diff_host_rate |
| 10  | hot                      | 24  | srv_count                | 38  | dst_host_srv_rerror_rate |
| 11  | num_failed_logins        | 25  | servr_rate               | 39  | dst_host_srv_rerror_rate |
| 12  | logged_in                | 26  | srvr_error_rate          | 40  | dst_host_rerror_rate     |
| 13  | num_compromised          | 27  | reror_rate               | 41  | dst_host_srv_rerror_rate |
| 14  | root_shell               | 28  | srvr_error_rate          |     |                          |

From these information, the algorithm will find patterns so that they can recognize which data is an intruder and categorized it into a threat. Moreover, the data that aren’t fit to be any types of attacks will be clustered as a normal class.

3.2. Measure for performance evaluation

Clustering will be done in binary classification procedure between class DoS and Normal, class Probe and Normal, class U2R and Normal, lastly class R2L and Normal. Firstly, the experiment will be performed by randomly choosing 10%, 20%–90% training data of total dataset and the remaining data will be used as testing data. In learning phase, data training will be used to build the model by finding the pattern of data input with clustering the data into 5 different classes which consist of four types of attack and Normal class. Whereas testing data will be used in evaluation phase to measure how accurate the constructed model. Hence, performance of KSPKM will be evaluated using the following formulation:

\[
\text{Accuracy} = \frac{\text{Total true prediction}}{\text{Total dataset}} \times 100\% \quad (7)
\]
4. Experimental results

We perform the first experiment using norm Euclidean function with the algorithm in Figure 1. Next, by implementing algorithm in Figure 2 for KSPKM, we tried to test using several different parameter values to seek the highest clustering accuracy model. All three experiments have been summarized in Table 2 below which containing the information of data training (DT) used, the best average clustering accuracy along with running time (RT) spent for each type of attack. For the kernelized version, we also added the parameter value that is $\sigma$ for RBF kernel and $d$ for polynomial kernel.

Table 2. Best accuracy results using spherical k-means with norm Euclidean function and kernel spherical k-means with RBF and polynomial kernel

| Data            | SPKM         | KSPKM        | RBF         | Polynomial |
|-----------------|--------------|--------------|-------------|------------|
|                 | DT (%)       | Accuracy (%) | RT (s)      | DT (%)     | Accuracy (%) | RT (s) | $\sigma$ | DT (%) | Accuracy (%) | RT (s) | $d$ |
| Normal-Dos      | 70           | 94,33        | 0,72        | 20         | 98,31        | 2,23 | 0,1     | 90     | 54         | 1,02   | 4   |
| Normal-Probe    | 40           | 95,09        | 0,25        | 10         | 97,04        | 0,27 | 0,00    | 60     | 95,24      | 0,47   | 6   |
| Normal-U2R      | 50           | 91           | 0,41        | 60         | 92,5         | 5,78 | 0,1     | 90     | 51         | 1,14   | 1   |
| Normal-R2L      | 80           | 84,5         | 0,64        | 30         | 88,71        | 3,05 | 0,1     | 60     | 52,38      | 0,86   | 5   |

As we can see from Table 2, SPKM clustered the data into four different types of attack or a normal class with the accuracy sets roughly between 84—95% and the best clustering accuracy achieved while using norm Euclidean function with 95,09% for Probe attack. Meanwhile it turns out that, operating KSPKM method using RBF and polynomial kernel resulting in a completely distinct result. It can be clearly seen that adding polynomial kernel to original SPKM algorithm has given an unstable clustering accuracy. Due to the fact that a proper outcome only shown while using KSKM to clustered Normal-Probe class that is reaching 95,24% average accuracy with $d = 6$. While in other cases, all three average clustering accuracies drastically dropped exceeding 40% to merely around 51—54%. On the contrary, RBF kernel generated a very satisfying result that is approximately between 88—98%. Additionally, with 0,1 parameter value, the best average accuracy (98,31%) attained by using 20% data training and 2,23 seconds running time spent to clustered data into Normal-Dos class.

5. Conclusion and future works

This research proposed a new method called Kernel Spherical K-Means (KSPKM) that has been modified from Spherical K-Means (SPKM) algorithm using kernel function as classifier for intrusion detection systems (IDS). We apply norm Euclidean for SPKM. Meanwhile, we applied both kernel RBF and kernel polynomial with SPKM for Kernel Spherical K-Means. We found out that Kernel Spherical K-Means with kernel RBF has perfected the clustering accuracy from the prior method which is SPKM. This is shown by producing a better result with the highest average clustering accuracy being 98,31% compared to SPKM that only achieve 95,09% highest accuracy value for clustering several types of attack.

Even though KSKM has been a very good method, we want to recommend another technique that might be considered to improve the performance for IDS. In future works we suggest to use another
clustering or classifier method such as Multiclass Support Vector Machines, Random Forest, etc. We also recommend to perform feature selection to reduce any redundant feature so that it can lessen the running time and storage usage in order to construct an even more efficient algorithm.

References
[1] Repalle S A and Kolluru V R 2017 Intrusion detection system using AI and machine learning algorithm International Research Journal of Engineering and Technology (IRJET) 4 1709—1715
[2] Rustam Z and Talita A S 2015 Fuzzy kernel c-means algorithm for intrusion detection systems Journal of Theoretical and Applied Information Technology 81 161—165
[3] Rustam Z and Zahras D 2018 Comparison between support vector machine and fuzzy c-means as classifier for intrusion detection system J. Phys.: Conf. Ser. 1028 012227
[4] Ikram S T and Cherukuri A K 2016 Intrusion detection model using fusion of chi-square feature selection and multi class SVM Journal of King Saud University 29 462—472
[5] Rustam Z 2010 Intrusion detection systems menggunakan fuzzy support vector machines Prosiding Seminar Nasional Matematika 2010 449—452
[6] Shi Z 2005 Efficient online spherical k-means clustering IEEE International Joint Conference 5 3180—3185
[7] Krismanti A, Rustam Z and Pandelaki J 2011 Aplikasi spherical k-means pada pengklasifikasian brain cancer Prosiding Seminar Nasional Matematika 2011 293—297
[8] KDD Cup 1999 Data, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
[9] Anderson J P 1980 Computer security threat monitoring and surveillance Technical Report James P Anderson Co. (Fort Washington: Pennsylvania)
[10] Paliwal S and Gupta R 2012 Denial-of-service, probing & remote to user (r2l) attack detection using generic algorithm International Journal of Computer Applications 60 57—62
[11] Ghaleb A M M and Talab S A 2013 Assembly classifier approach to analyze intrusion detection dataset in networks by using data mining techniques International Journal of Science and Research (IJSR) 4 742—748
[12] Kaushik S S and Deshmukh 2011 Detection of attacks in an intrusion detection system International Journal of Computer Science and Information Technologies (IJCSIT) 2 982—986