Revisiting Recent and Current Anomaly Detection based on Machine Learning in Ad-Hoc Networks

Zhixiao Wang\textsuperscript{1,2,3,4}, Mingyu Chen\textsuperscript{2}, Wenyao Yan\textsuperscript{5}, Wendong Wang\textsuperscript{6}, Ang Gao\textsuperscript{7}, Gaoyang Nie\textsuperscript{1}, Feng Wang\textsuperscript{1}, and Shaobo Yang\textsuperscript{1}

\textsuperscript{1} Xi’an University of Technology, Xi’an 710048, China
\textsuperscript{2} Goettingen University, Goettingen 37077, Germany
\textsuperscript{3} Xi’an Jiaotong University, Xi’an 710049, China
\textsuperscript{4} Shaanxi Provincial Key Laboratory of Network Computing and Security Technology, Xi’an 710048, China
\textsuperscript{5} College of Xi’an Innovation, Yan’an University, Xi’an 710100, China
\textsuperscript{6} Yan’an University, Yan’an 716000, China
\textsuperscript{7} National Satellite Meteorological Center, China Meteorological Administration, Beijing 100081, China

Email: wangzx@xaut.edu.cn, mingyu.chen@stu.uni-goettingen.de, yadxwwd@163.com

Abstract. Ad-Hoc network which is one kind of self-organized networks is much more vulnerable than the infrastructural network with the properties of highly changeable linkage, dynamic structure, and wireless connections so that the tradition intrusion detection system (IDS) should be improved to adapt in such network with limited computing resources and open channels. To ensure the security in Ad-Hoc network, the efficient anomaly detection methods should be probed. Over the past years, many studies have implemented anomaly detection methods (intrusion detection techniques) based on machine-learning methods in this field. This article analyzes the existing security problem in Ad-Hoc network, presents the basic theory of intrusion detection for Ad-Hoc network, and reviews the current and recent anomaly detection methods used machine learning techniques in the intrusion detection system.

1. Introduction

Nowadays, the internet has been an essential component of our daily life. Terabytes of data pass through the internet network. The data may contain the confidential information of the individuals, companies or even countries. Thus, how to ensure the security of the internet from a variety of attackers and incident breakages should be a great issue. Especially in Ad-Hoc network, the attack techniques can be more changeable and unpredictable which makes the detection of the intrusion more difficult. In this paper, we will first discuss the security issues in Ad-Hoc network, and review some techniques of anomaly/intrusion detection that have been suggested in Ad-Hoc networks. In addition, we will introduce the basic theory of the intrusion detection system and some recent and current methods which can be utilized to realize the layered intrusion detection system for Ad-Hoc networks. What’s more, we will investigate some machine learning methods and the popular deep learning method based on Generative Adversarial Network (GAN), which can be applied in the intrusion detection system.

As the properties of the Ad-Hoc Network, it has plenty of advantages such as flexibility, extensibility and self-organization [1]. However, compared to the traditional fixed network, more security issues appear in the Ad-Hoc Network because of its dynamic and vulnerable network structure [2].
attackers can be external intruders, attackers outside the network and internal intruders, attackers have the authenticated identity inside the network.

- Owing to each node in Ad-Hoc Network transmits the packets via the wireless channels, it is much easier for the attackers to eavesdrop, distract and manipulate these nodes.
- As the Ad-Hoc Network is composed with client devices dynamically, attackers can easily join the network and eavesdrop the information. It is hard to discriminate the malicious attackers from the normal users in the network. The firewall is also not suitable in such rapidly changing network.
- Considering the Ad-Hoc Network’s properties of dynamic network topology, the location change of the cellular may cause the broken linkage. In addition, the transmission of routing protocol may leak the location information of the users and the attackers can hide themselves easily in the network by changing the physical location.
- As the nodes of Ad-Hoc Network are widely separated and in most condition are mobile, they are easier to be broken physically.
- As the Ad-Hoc Network is decentralized, there is no designated certification centre for encryption. The traditional public key encryption technology for infrastructure network cannot be used in such system.
- To realize the routing protocol, nodes in the network need to collaborate in data transmission. The attenders have no guaranteed resource to transmit the data package which may cause the package loss and the link breakage.

The rest in the paper is scheduled as follows: In Section 2, related works of Intrusion Detection Techniques for Ad-Hoc networks are reviewed. Traditional Machine Learning Methods for Anomaly Detections in Ad-Hoc networks are represented in Section 3. Deep Learning Methods for Anomaly Detections including GAN (Generative Adversarial Networks) are shown and discussed in Section 4. Finally, Section 5 concludes the paper and presents the future works.

2. Intrusion detection in Ad-Hoc network

As the Ad-Hoc network has the properties of infrastructureless, low-speed communications, limited bandwidth and energy source, the change and disconnection between user ends become more usual. In addition, the speed of analyzing and alerting should be slower in a decentralized network. Thus, the intrusion detection system for the traditional network should be modified in the Ad-Hoc network. Since the Ad-Hoc network doesn’t have the router to deploy the network-based IDS, a method to solve this problem is to elect the temporary center for the nodes in a specific area.

In the previous research, most IDS for the Ad-Hoc network is improved relied upon the traditional distributed intrusion detection system [7, 8]. A literature [7] has proposed a Zone-based intrusion detection system which divided the network into the non-overlapping areas based on physical locations. Nodes in each zone are divided into gateway nodes and normal nodes. Each gateway node can interconnect with the other gateway nodes outside its own zone, and normal nodes only interconnect with nodes inside its zone. IDS agent on each node monitors its behaviors. Data are gathered by each gateway node to analyze the communication behavior and if the anomaly is detected, the location of each malicious node will be broadcast to the whole nodes in the area. This strategy is relied upon the idea of the hierarchical Ad-Hoc network, which gathers the clusters and chooses the temporary “center” for each cluster. Each temporary center may work as a base station with network-based IDS to analyze the communication data and has the responsibility to detect the anomaly and broadcast the malicious attack to each device in the cluster. However, in my opinion, the selection of the gateway node may be too rough without consideration of the computing resource of each end device. There are more related researches for the center election of the cluster. Considering the features of Ad-Hoc networks, Energy Aware Clustering Algorithm which elect the center of the cluster according to energy storage and mobility status of nodes has been proposed [20]. The Link Expiration Time (LET) measures the
mobility status of the node which is related to the parameters of speed, direction and propagation range of the node. The center of the cluster should have more energy and the larger average value of LET which improve the anomaly detection accuracy by reducing the linking failure caused by the mobility of the nodes or the lack of energy. In article [9], the authors have proposed a new election method using the Vickrey-Clarke-Groves scheme based on Bayesian game to select the cluster leader in MANETs for hybrid IDS, which successfully reduce the congestion in the intrusion detection system and network power consumption.

3. Traditional Machine Learning Methods for Anomaly Detections

Machine learning methods used in the anomaly detections are often categorized into three subtypes: supervised learning, unsupervised learning, and reinforcement learning.

- **Supervised learning methods** require the given dataset to be labeled as the anomaly or not. The most popular supervised learning methods include Support Vector Machines (SVM), linear classifier, logistic classifier, naïve Bayes, decision trees, k-nearest neighbor (KNN), Neural Networks, etc., which are used to classify the given cases as normal or not.

- **Unsupervised learning** do not require the dataset to be labeled. There is a hypothesis when using unsupervised learning methods that most of the cases in dataset is normal and the task for the algorithms is to find the outliers. The most popular unsupervised learning algorithm is clustering includes hierarchical clustering, k-means, mixture models, DBSCAN and OPTICS algorithm. Reinforcement learning methods learn from the environment and give the labels to the unlabeled data [3].

- In anomaly detection field, comparing the similarity between the tested set with the trained model for normal instances to recognize the possibility of being anomaly case is a semi-supervised anomaly detection methods [4].

Nowadays, to advance the IDS performance, machine learning techniques are implemented in intrusion detection issues. According to a survey [3], the most widely used machine learning methods in the intrusion detection system are Naive Bayes, Decision Tree, Support Vector Machines, K-means, and Artificial Neural Network. We will introduce those common popular algorithms.

3.1. **Support Vector Machines**

Support Vector Machines (SVM) classifier is a supervised machine-learning method which is suitable for binary class issues. It builds a non-probabilistic binary linear classifier to approximate the true model of the given dataset. All the data points in sample dataset will be divided into two separated space. A hyperplane will be trained to separate these two categories. As there will be infinite candidate hyperplanes in the gap, the model is optimized by improving the margin between two classes and reduce the generalization error [5]. As the given data for network status is not always continuous, Support Vector Machines classifier can also deal with the data with non-linear elements with kernel function to project the data point into higher dimensional space. With the trained model, the new given point can be easily put into two categories. Support Vector Machines classifier has a great performance in the comparatively small dataset with high dimension vector and it also has high efficiency in making the decision. As there will be a huge amount of features in the Ad-Hoc network analysis, Support Vector Machine can be a good choice for two-class classification. The variant One-Class Support Vector Machine can be applied in anomaly detection. The disadvantages of Support Vector Machines is if the training dataset is huge, it will take a lot of time to train the model and commonly, it is a binary classifier which cannot identify different types of attack in intrusion detection.

3.2. **Decision Tree**

Decision tree classifier builds decision tree depends on the train data. The tree model is readable and explainable. It is built by dividing the value of given features. The basic rule for generating a tree
model is ensure the entropy to reduce as fast as possible from the tree stump to the leaf. The theory of decision tree is to find the partition method with highest purity. The purer the tree is, the less entropy. There are several algorithms to calculate impurity such as ID3, C4.5 and CART [6]. The tree stump is the most important feature and the leaf node is the final label. James Zhang has compared the use of decision stumps and decision trees in anomaly detection and the performance of the decision stumps applied to BDT (Boosted Decision Trees) works more efficient in practice [10]. Decision tree performs well in multi-class classification which is suitable for the labeled network dataset with various kinds of intrusion. Random forest classifier, the improvement method of decision tree usually has better result. More trees will be generated with the random sampled data and the input will get labeled class by voting. Decision tree is suitable for training huge dataset and experiment result is usually accurate. However, it may take long time in constructing a decision tree.

3.3. Na"ive Bayes
Na"ive Bayes classifier use the Bayes formula to calculate the probability for the label of input data with certain features. Then choose the label with highest probability as the final result. There is a hypothesis of this algorithm that each feature is independent. Na"ive Bayes classifier is a multi-class classifier which can be used to separate the category of different attacks and it cost little computer resource. This method is more suitable for the data that features are less related.

3.4. K-means
K-means is the clustering algorithm of unsupervised machine learning method. Analyzer needs to set k initial centroids as the number of labels. The sample point will assign to the cluster according to the distance between the point and the centroids. Then the centroids will be recalculated. The classification will be finished until the centroids do not change anymore. The quality for the cluster can be evaluated with sum of the squared error. This method can deal with the unlabeled dataset and recognize the unknown intrusion in the Ad-Hoc Network. Fei Huan has applied K-means in anomaly detection for WSN and found it perform better than Density-based Spatial Clustering of Applications with Noise (DBSCAN) for larger dataset [11]. Zhang Duan has proposed a clustering scheme depended upon K-means and QPSO which is proved to be effective for wireless network anomaly detection [12]. It can also be used to preprocess the dataset to summarize the feature of different attack and use other methods to assign the labels.

3.5. Artificial Neural Network
The artificial neural network is the simulation of the human’s brain. It is usually used to approximate rule in nature or the representation for the logic strategies. The model is composed of a huge amount of nodes which can be called neuron. Each neuron represents a specific activation function and the connection between two nodes represents the weight. An artificial neural network can be classified into three layers: input layer, hidden layer, and output layer. The training process of artificial neural network for classification is to contradistinguish the difference between the output and the expected label, feedback the error to the former nodes and update the weight to gain better results. There are many supervised and unsupervised study rules for the model such as back-propagation, a typical supervised study rule. The artificial neural network has the ability to extract the feature from the input. Thus, as the input of the network data is massive and hard to manage feature, the artificial neural network can be a good choice. However, using an artificial neural network in real time IDS may be a great challenge considering its huge consumption in training the model.

The following table 1 shows the supervised detection accuracy of those machine learning methods. The training and testing dataset is KDD99, a dataset has 21 kinds of attacks and 41 variable for training. All the methods achieve good detection accuracy over 90 percent. Without feature management, random forest algorithm achieves the best result.
Table 1. Performance of different machine learning methods on the KDD99 dataset [24][25][26].

| Model   | Accuracy  |
|---------|-----------|
| SVM     | 0.9299    |
| DT (J48)| 0.9310    |
| RF      | 0.9377    |
| NB      | 0.9123    |
| ANN     | 0.9190    |
| K-means | 0.9102    |

4. Deep Learning Methods for Anomaly Detections

4.1. Generative Adversarial Networks

As the Ad-Hoc network is vulnerable, there will be plenty of unknown anomalies occur. The neural network has the ability to extract features from random input which can be used in unsupervised learning for anomaly detection. Here we will introduce an advanced model consists of neural networks which is much efficient to be applied in real-time IDS.

Generative Adversarial Networks is one of the deep learning methods which is proposed by Ian J. Goodfellow with the aganippe, two-player game. Deep learning method has great advantages in handling high-dimension dataset. GAN is composed of two training models, a generative model, and a discriminative model, which is shown in Figure 1. Suppose the samples from the training data have their own distribution of feature. The task of the generative model is to try to simulate the features of the real data and generate fake samples with random input noise as real as possible. The task of the discriminative model is to estimate the probability of the input which contains samples both from real data and generated fake data from the generator to be real. In other words, the generator is trying to deceive the discriminator [16].

In the training process, two models are trained alternately, as shown in Figure 2. Keep one and update the weight of the other model. Generator and discriminator both optimize themselves to compete with each other until reach a dynamic balance (Nash equilibrium).

This algorithm can be learned as a maximum and minimum problem. The generator G tries to make the discriminator D consider its input from G as the real data and D tries to make the output probability to be true of input generated data as zero. When training discriminator, the value of the function should be optimized to be maximum. The former formula represents the probability to be true with the real data input. If the input is generated data, the discriminator wishes the minimum value which has a conflict for the whole function to gain extreme value. Thus, the second formula is modified as one minus the output probability with generated input. To optimize the generator, we want to gain the minimum value of second formula.

$$\min_G \max_D V(D, G) = E_{x \sim p_{data}(x)}[\log D(x)]$$ (1)
4.2. Efficient GAN in Anomaly detection

As GAN has the ability to simulate the distribution of the input data, GAN can be used in anomaly detection by learning the feature of the normal data with the generator and the discriminator can be used to recognize the anomaly. The generator creates latent space for the given normal dataset with distribution \( p \). If a new normal sample is given, it should have a corresponding point in the latent space. Otherwise, the input sample is abnormal [14].

According to Houssam Zenati [15], in practice, if we want to applied deep learning method in IDS for anomaly detection, the problem of the high cost of the time should be resolved. The procedure to optimize the GANs takes a long time with a huge dataset which may not fulfill the requirement of real-time system. To solve this problem, Zenati introduces an encoder into GANs which can map the input sample \( x \) into latent space to save the computational resource. The input in latent space is represented as \( z \). This improved GANs can be called BiGANs which is developed with inference model [17]. As the figure 3 is shown, the input of discriminator is a joint (data, latent) pairs.

\[
+ E_{z \sim p_z(z)}[\log(1 - D(G(z)))]
\]

\( (2) \)

The task of the discriminator is to distinguish the input from generator and its noise source or the encoded input from real dataset and the original real data sample. As the encoder is included in the GANs, the value formula to be optimized can be represented as follow.

\[
V(D, E, G) = E_{x \sim p(x)}[E_{z \sim p_z(z)}[\log D(x, z)]]
\]

\( (3) \)
\[ + E_{z \sim p(z)} [ E_{x \sim p_G(z)} [ \log(1 - D(x, z)) ] ] \]  

(4)

To estimate the anomalous level of the input, Zenati defines a formula \( A(x) \) which composed of reconstruction loss and discriminator-based loss defined as follow. Zenati proposes two definitions for discriminator-based loss. One is the cross-entropy loss which calculates the confidence of the discriminator that input is from the real dataset. The other is called feature-matching loss which evaluates the similarity of the features between the generated data and the real data. The larger the value of \( A(x) \) is, the more anomalous the input sample is.

\[
A(x) = \alpha L_G(x) + (1 - \alpha) L_D(x)
\]

(5)

Reconstruction loss:

\[
L_G(x) = \| x - G(E(x)) \|_1
\]

(6)

Discriminator-based cross-entropy loss:

\[
L_D(x) = \sigma(D(x, E(x)), 1)
\]

(7)

Discriminator-based feature-matching loss:

\[
L_D(x) = \| f_D(x, E(x)) - f_D(G(E(x)), E(x)) \|_1
\]

(8)

As the deep learning method is good at solving the high-dimension problem, Zenati applies the GAN on MNIST to evaluate the performance of the improved GAN with encoder. To evaluate the GAN in anomaly detection, KDD99 free dataset is used in the experiment. The dataset is divided in half for training and testing randomly. Only normal data from train dataset is used for training. The 20 percent of samples that achieve highest \( A(x) \) score will be considered as anomalies. The evaluation matrixes are precision, recall, and F1-score. Before the experiment, Zenati handles the categorical feature with a one-hot representation method and also use the min-max scaling method to standardize the numerical features. The experiment is implemented with Tensorflow. The result of the improved GAN is compared with AnoGAN and some previously proposed models as the table 2 shown. The improved GAN has the best performance in recall and F1 matrix with discriminator-based cross-entropy loss.

| Table 2. Summary of Performance on the KDD99 dataset [15] |
|---|---|---|---|
| Model | Precision | Recall | F1 |
| OC-SVM | 0.7457 | 0.8523 | 0.7954 |
| DSEBM-r | 0.8521 | 0.6472 | 0.7328 |
| DSEBM-e | 0.8619 | 0.6446 | 0.7399 |
| DAGMM-NVI | 0.9290 | 0.9447 | 0.9368 |
| DAGMM | **0.9297** | 0.9442 | 0.9369 |
| AnoGAN\(F_M\) | 0.8786±0.0340 | 0.8297±0.0345 | 0.8865±0.0343 |
| AnoGAN\(\sigma\) | 0.7790±0.1247 | 0.7914±0.1194 | 0.7852±0.1181 |
| Zenati et al \(Model_{F_M}\) | 0.8698±0.1133 | 0.9523±0.0224 | 0.9058±0.0688 |
| Zenati et al \(Model_{\sigma}\) | 0.9200±0.0740 | **0.9582±0.0104** | **0.9372±0.0440** |

Zenati et al. also compare the inference time of the improved GAN and AnoGAN and the result shows that the improved GAN runs 700x to 900x faster than the AnoGAN, which is shwown in table 3. As we can see, the inference time with improved model is accelerated to be in 3 (ms). The efficient deep learning model GAN can be used in real-time IDS to detect the anomalies.
Table 3. Average inference time over 100 batches (ms) [15]

| Dataset        | $L_D$ | $\sigma$ | AnoGAN | BiGAN | Speed Up |
|----------------|-------|----------|--------|-------|----------|
| 2*KDD          |       |          | 2578   |       | 2.7      | 950     |
| FM             |       |          | 3527   |       | 5.3      | 660     |

5. Conclusion
This paper reviews the security problems in Ad-Hoc networks and basic techniques used in intrusion detection. Optimization of the intrusion detection system from traditional one should concentrated on the specific routing protocol in the Ad-Hoc Network, resource limitation of devices, the vulnerability of linkage and the decentralized structure. As the nodes in the Ad-Hoc network can be clustered, the algorithms to select the cluster leader can be a good solution to resolve the problems. We also introduce the machine learning methods widely used in the intrusion detection system and analyze the advantages and disadvantages of them. An efficient deep learning method, Generative Adversarial Network is explained in detail which can be applied to a real-time system with highly optimized speed. As many machine learning methods have been accepted in the intrusion detection system, more attention needs to be paid on feature selection and improvement of algorithms to defend the system from the various attacks.

6. Acknowledgment
The work is supported in part by the grants which include: Scientific Research Program Funded by Shaanxi Provincial Education Department (Program No.16JS080), College Innovation Research and Development (No. 2016JXY-20), YAN’AN Science and Technology Project (No. 2018KG-02), Xi’an Science technology (No.2017080CG/RCC043(XALG027)), the CSC201608615074, NSFC (No.61772407, No.61771387), Youth Fund of the Ministry of Education of China (No.16YJCZH109), Shaanxi Social Science (No.2014M18), Shaanxi Department of Education (No.18JXK1216), CERNET Innovation Project (NGII20171202, NGII20170303), Ph.D Innovation (No.112-45115006), College Innovation Research and Development (No.310/252051835).

7. References
[1] Corson, J.Macker 1999 Mobile Ad-Hoc networking (MANET): Routing protocol performance issues and evaluation considerations [S] RFC 2501.
[2] Zhou L, Haas Z. J. 1999 Securing Ad-Hoc networks[J] IEEE network 13(6) 24-30.
[3] Haq N F, Onik A R, Hridoy M A K, et al. 2015 Application of machine learning approaches in intrusion detection system: a survey[J]IJARAI-International Journal of Advanced Research in Artificial Intelligence 4(3) 9-18.
[4] Varun Chandola, Arindam Banerjee, Vipin Kumar 2009 Anomaly detection: A survey ACM Computing Surveys (CSUR) 41(3) 1-58.
[5] Trevor Hastie, Robert Tibshirani, Jerome Friedman 2009 The elements of statistical learning: data mining, inference, and prediction (Berlin: Springer).
[6] Lior Rokach, O. Maimon 2008 Data mining with decision trees: theory and applications. World Scientific Pub Co Inc. ISBN 978-9812771711.
[7] GONG Yuanynan 2012 A kind of intrusion detection system of wireless Ad-Hoc ethernet based on domain Computer Engineering and Applications 48(28) 123-126.
[8] Y. Zhang W. Lee 2000 Intrusion detection in wireless ad-hoc networks Proceedings of the 6th annual international conference on Mobile computing and networking 275-283.
[9] Subba, B., Biswas, S., Karmakar, S. 2016 Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation Engineering Science and Technology, an International Journal 19(2) 782-799.
[10] J. Zhang, , Vukotic, L., Gardner, R. 2018 Anomaly detection in wide area network mesh using two machine learning anomaly detection algorithms CoRR 1801-10094.
[11] Fei Huan, Li Guanghui 2015 Abnormal Data Detection Algorithm for WSN Based on K-means Clustering[J] Computer Engineering 41(7) 124-128
[12] ZHANG Duan, LIU YuanHAO Jian-dong 2010 Network anomaly detection based on fuzzy clustering algorithm and QPSO algorithm in mobile Ad-Hoc Computer Engineering and Applications 46(30) 92-94.
[13] Kumar, G. 2014 Evaluation metrics for intrusion detection systems—a study International Journal of Computer Science and Mobile Applications, Evaluation 2(11) 11-17.

[14] Lucas Deecke, Robert Vandermeulen, Lukas Ruff, Stephan Mandt, Marius Kloft 2018 Anomaly Detection with Generative Adversarial Networks ICLR 2018 Conference.

[15] Houssam Zenati, Chuan Sheng Foo, Bruno Lecouat, Gaurav Manek, Vijay Ramaseshan Chandrasekhar 2018 Efficient GAN-based anomaly detection CoRR preprint arXiv:1802.06222.

[16] Roman Trusov 2016 GAN Deep Learning Architectures – review. [ONLINE] Available at: https://sigmoidal.io/beginners-review-of-gan-architectures/. [Accessed 7 January 2019].

[17] Jeff Donahue, Philipp Kraehenbuehl, and Trevor Darrell 2017 Adversarial feature learning International Conference on Learning Representations (ICLR 2017) arXiv:1605.09782.

[18] Creswell, A., White, T., Dumoulin, V., Arulkumaran, K., Sengupta, B., Bharath, A. A. 2018. Generative adversarial networks: An overview IEEE Signal Processing Magazine35(1) 53-65.

[19] Anonymous 2018 What is IDS and IPS?. [ONLINE] Available at: https://www.juniper.net/us/en/products-services/what-is/ids-ips/. [Accessed 11 January 2019].

[20] Y. Xu and W. Wang 2006 MEACA: Mobility and Energy Aware Clustering Algorithm for Constructing Stable MANETs IEEE Military Communications conference 1-7 (Washington:DC).

[21] Thomas, A. K., Devanathan, R. 2012. Variable duty-cycle based efficient network discovery in WSN European Journal of Scientific Research 93(2) 266-278.

[22] Sebastian Schaal 2017 Generative Adversarial Networks (GANs). [ONLINE] Available at: https://wiki.tum.de/pages/viewpage.action?pageId=23562510. [Accessed 13 January 2019].

[23] Roman Trusov 2017 GAN Deep Learning Architectures – review. [ONLINE] Available at: https://sigmoidal.io/beginners-review-of-gan-architectures/. [Accessed 13 January 2019].

[24] Almseidin M, Alzubi M, Kovacs S, Alkasassbeh M 2017 Evaluation of machine learning algorithms for intrusion detection system IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY) 277-82.

[25] Hasan MA, Nasser M, Pal B., Ahmad S. 2014 Support vector machine and random forest modeling for intrusion detection system (IDS) Journal of Intelligent Learning Systems and Applications 6(01) 45.

[26] Chandrashekhar AM, Raghuveer K. 2012 Performance evaluation of data clustering techniques using KDD Cup-99 Intrusion detection data set International journal of information and network security 1(4) 294.