Fusion of Artificial Neural Networks by Fuzzy Logic Based Attack Detection Method

Adel Dallali, Takwa Omrani and Belgacem Chibani Rhaimi

November 10, 2021

Fusion of Artificial Neural Networks by Fuzzy Logic Based Attack Detection Method

Adel Dallali
University Of Gafsa
2100, Gafsa, Tunisia
adel.dallali@gmail.com

Takwa Omrani
ENIG/MACS University of Gabes
Rue Omar Ibn Elkhattab, 6029 Gabes,
Tunisia. omranitakwa@yahoo.fr

Belgacem Chibani Rhaimi
ENIG/MACS University of Gabes
Rue Omar Ibn Elkhattab, 6029 Gabes,
Tunisia abouahmed97@gmail.com

***Abstract*—** One promising method for improving the performance of fuzzy logic theory attacks and intrusions detection consists in using an appropriate classic data fusion method that detect and estimate an attack in reel TCP/IP connection. This paper, a method of combining multiple artificial neural network based on fuzzy logic, is presented, particularly the fuzzy integral that is able to predict a real TCP/IP connection as normal or suspicious one.

The central idea of this method is to separate a great large dataset into a number of sub-datasets. Then, each sub-dataset will be trained and tested with a different artificial network. Hence, all results from multiple ANN decision will be fuzzed by using the fuzzy logic algorithm. Experiments have been conducted with several network samples selected from NSL-KDD DARPA dataset. Empirical results improve that performing fuzzy logic data fusion techniques is a promising direction for cyber-attack detection.

Keywords*— *Attack, Cybercrime, Data fusion, fuzzy logic

I. INTRODUCTION

Recently, various attacks and intrusions forms was appeared and caused significant social and financial problems. As example, viruses, fishing, theft of data, carding, financial fraud, etc [1]. A consequence, attack detection is becoming challenging task for recent researches. for example, TCP/ IP connection attacks is one of electronic cyber-crime types that intends to break the confidentiality, integrity and/or availability of the data be it an online traffic or in the local host [2].

Internet Detection Systems (IDSs) identifying malicious attacks in order to protect computer systems from possible damages.

An IDS is a mechanism that identify activities abnormal or suspicious on the analyzed target (a network or host). It allows having a preventive action on the risks of intrusion. But, an attack can be the main function of an IDS is identifying malicious attacks in order to protect computer systems from possible damages.

It often uses a mechanism that listens to network traffic in order to identify abnormal or suspicious activities and thus to have a prevention action on intrusion risks.An attack can be made either by a single source or by several sources, where multiple programs coordinate to launch their attacks simultaneously. But, some anonymous sources of attacks stilled hard challenges [3] for IDS. Sometimes, if the source of data is unknown or imperfect, it is impossible for IDS to different between “safe” and “dangerous” connection [4].

Hence, IDS’s attack detection accuracy of system can be decreased and the false positive rate of detection stays high even though the average of accuracy stays low [5].

The main reason of this limitation is, that, most of developed attack detection approaches rely especially on a limited set of attacks. That is why; they cannot detect some attacks when samples of information are ambiguous or imperfect. For this reason, few approaches started investigating toward this direction.

To overcome this problem, various intrusion detection systems have been proposed in the literature. The main difference is the use of the appropriate techniques to analyze the data in order to investigate the existence of an attack. To decrease attack detection problem, machine learning (ML) techniques have been recently proposed in attack detection rate and to involve the administration of IDS. ML method builds models from training data because it can dealing with anomaly and intrusion detection as a classification challenge.

Many ML based approaches have been suggested in the literature that can give a major flexibility [5], [4] in detection network connection attack.

Both approaches of research in attack detection and analysis are still too much concentrated on estimating intrusion in a certain environment [6]. But, if the network features given are ambiguous or imperfect, these methods become insufficient for the detection of attacks.

This concept has been the basic aim of our classic data fusion system. Our work is about the use an efficient strategy that can support ambiguous data and improve the decision of information’s state with a limited error rate.

Following this trend, new attack detection approach have been emerged and explored in [7],[8]. But, these approaches still suffer from the lack of sources of information. Data fusion approaches are crucial to network connection classification problem. From this perspective this work lies at the attack and intrusion analysis which are recently being increasingly researched.

In this paper, we propose a multiple artificial network Fusion using Fuzzy logic fusion theory presented on a great large dataset. Our experimentation results are validated by we evaluating our approach on the real benchmark of TCP connections labeled in DARPA KDD99 dataset [9]. Our results improve that combining ANN classifiers with fuzzy

logic decisions can degrade the error rate of attack detection. The rest of the paper is organized as following: section II states different attack analysis and detection approaches. In section III, we show classification results of fuzzy logic then we compare its performance with existing approaches. Finally, we achieve our paper by a short conclusion and futures works.

II. Related Work

Many approaches have been proposed to investigate attack detection problem within online network connection. Machine learning methods are the most ones that have been used in [10]. Theses method can be supervised approaches [11] unsupervised approaches [6] to hybrid ones [7], [8].

Supervised approaches decide the class of network connection by using a several range of samples and labeled data for training attack classifiers. For example, Haddadi et al. [12] proposed detection method that use artificial neural network with back propagation algorithm for network based intrusion detection. This model conducts the KDD-CUP99 dataset for a binary classification of network attacks. In the same context, Haidar et al. [13] explored attack-based detection system by performing a supervised neural networks classifier to improve the efficiently of intrusion system. The first vulnerability is the luck of a training benchmark that makes the classification algorithm more complex. In addition, dealing with significant features can be a challenge and, where the information sources are unbalanced, the training sets may include some noises that make false alarm rates more increased.

To tackle this problem, other authors proposed the use of unsupervised approaches to make attack detection more flexible task. For instance, Chandola et al. [14] suggest using a support vector machine (SVM) classifier for attack detection process. In this context, Markov model-based intrusion detection system is used by Moor Andrew [15] to calculate the probability of attacks existed in the system. This algorithm is based on a list of observations. For example, a list of alerts from an intrusion detection system (IDS) such as Snort can be used to determine the probability of system being attacked.

In other hand, Bronstein Alexandre et al. [16] proposed networks model for intrusion detection based on a Bayesian probability. In the same context of unsupervised method, K-means clustering technique is used by Imam Riadi et al. [17] and have been tested in order to range attack in TCP and UDP connection into three classes respectively “dangerous”, “rather dangerous” and “not dangerous” attack. However, this method cannot support a huge number of intrusion scenarios.

However, unsupervised classifiers can deal only with training of normal attack. Hence, a minimal deviation is considered as an attack. This algorithm involved weakly in attack detection, that is, the number of false positive rate remains increased. Then, by using one algorithm (supervised or unsupervised) of classification of the network traffic data as normal behavior or anomalous, can give a low attack detection accuracy with important alarm rate.

Hence, in this state, hybrid approaches ban be an optimal solution, in where both supervised and unsupervised methods decisions, are combined. For instance, M. Elbasiony et al. [7] proposed an hybrid IDS by using two famous data mining algorithms that are random forests and k-means. Similarly, Panda et al. [8] explored an hybrid attack detection algorithm that merge Decision Trees, SVM and Random Forest algorithms, that aims to classify network attack. However, these techniques suffer from identifying all attacks attempts, that as, this solution is failed at achieving a higher detection rate and lower false alarm rate. In iddition, Tsujii [18] tried to use the Naive Bayes classifier combined with the well-established EM algorithm to exploit the ambiguous data. In other works, Naive Bayes and decision tree classifiers were merged for network intrusion detection which given high accuracy for different scenarios of network [19].

On the other hand, Hurley et al have explored the use of statistical methods [20], and data mining technique have been used, examining how user profile features can be integrated into the system database to increase the accuracy of network attack classification. But, this approach may be insufficient if produce effective attack if users profiles are statistically identical.

Similarly, [21] have proposed and evaluated an attack detection algorithm based on statistics and behavior of user.

However, no previous studies have highlighted on investigating attack detection of a great large database. Recently, classic data fusion technique as probability, fuzzy logic and evidence theory was been recommended to be applied when data source are ambiguous numerous that as these technique does not requires a training phase.

In this trend, the method of multiple neural network model Fusion using Fuzzy system presented by this paper is an effective method of dealing with a great large dataset to improve the detection performance of fuzzy logic intrusion detection system. Then, we compare the empirical result with other intrusion detection developed in the literature. We understand that the proposed fuzzy logic multi-sensor data fusion IDS is able to contribute the attack detection process.

III. Attack Detection Analysis of Network Connection.

A. Data Description

MIT Lincoln was developed KDD’99 TCP connection corpus, from this large dataset, the NSL-KDD subset was developed [9]. The objective is to eliminate the redundancy founded in version of DARPA datasets (KDD99, KDD’2000) that can break the accuracy of our experimentation [13]. The labeled dataset is chosen for attack classification method. Network attack are grouped

into four classes : (i) Denial of service (Dos), where some resource is emerged, causing DoS to safe users.(ii) Probes which is collecting network information to avoid security tools. (iii) Remote to Local (R2L) attacks that use remote system vulnerabilities to penetrate a system. (iiii) User to root (U2R) attacks that aims to gain root access to a system. A part samples containing 10000 samples is randomly selected. In our work, we are interested only at binary classification of connection, then two labeled classes are presented; "attack" with score 1 and "normal" with score 0. The selected subset consists of 125374 feature collected from the 58530 for attack class and 67353 for normal class [9].

B. Data Preprocessing

Attack detection is based on a finite number of sensors. These sensors mean the attribute that forms the NSL-KDD database. To make our dataset more flexible to dealing with our proposed algorithm, a preliminary cleaning step of the database used is required. This stage consists of four main phases.

1. If the number of sample is more than 500, the distribution of the connection states in the base NSL-KDD is not equilibrated. Probes (11656 instances) attack is dominated in this case.
2. Denial of Service (DOS) attacks (45,927 instances) are also several and redundant. That is why, it is necessary to eliminate some of these attacks to realize balance with other attacks classes like R2L (52 instances) only and U2R (995).
3. The attack data is divided into two disjoint partitions containing only attack and normal types. Hence, the selected data is decomposed into three separated sets: the training data, the validation data and test data.
4. To efficiently evaluate our proposed algorithm, we randomly selected 1000 instances for validation and testing. Then, we imposed a 50% attack rate to maintain the balanced distributions of attack types. An example of reducing and standardized data is shown in the table 1.

@IP source	@IP destination	flag	class
0.282	0.0351	0.9970	0
0.3180	0.3305	1.3382	1
0.0280	0.0462	1.2255	0
0.3180	0.3305	0.8434	1
0.0280	0.1127	0.3632	0
0.0282	0.0714	1.3405	0
1.4425	3.2210	1.4527	1

Table 1: Example of Used Dataset

The objective of our approach is to take NSL-KDD dataset features as input and predict the attack score of each of connection mentioned in dataset sample. Attack score needs to be floating point values in the range of 0 (normal connection) to 1 (attack), with 0,5 designating suspicious connection. Some of the used dataset features are not important for detection process. For this, a feature extraction task is required.

IV. FEATURE EXTRACTION

For each connection instance, a feature-vector is prepared by using the j-48 tree decision based algorithm that we shows three more significant feature that can be significant to be used in the estimation attack process. Then, NSK-KDD dataset is converted to three column matrixes that contains tree feature which are @IP-source, @IP-destination and flag feature. The following table 1 shows the created matrix with new selected features.

actual class	**normal class**	**attack class**
normal class	TP	FP
attack class	FN	TN

TABLE 2: COVARIANCE MATRIX

Where:
TP: Number of features that is well classified as normal.
TN: Number of feature that is well classified as Intrusion.
FP: Number of feature classified as intrusion but they were normals.
FN: Number of feature classified as normal but they were attacks.
To improve the performance of classifiers, two criteria were used as demonstrated namely TP rates and FP rates.

V. FUZZY LOGIC THEORY

Fuzzy logic theory was proposed by Dr. Lofti Zadeh [22] in 1965 as a tool of processing ambiguous or noisy data. After ten years that fuzzy theory was invented, Dr. E. H. Mamdani, who was applied the fuzzy logic in controlling an automatic steam engine in 1974 [23].
Recently, the Mamadani fuzzy logic efficiency has been conducted in many researches application [24]. For instance, in semantics data [25], in online communities [26] and in detecting unfair rating [27]. A fuzzy logic concept takes inaccuracies and uncertainties challenges of data source into account. So that, it provides a very valuable flexibility for reasoning by dealing with partial set membership rather than crisp set membership.
Let S be the universe, or reference space. We denote by x, y, etc. its elements (or points).
A subset x of S is defined by its characteristic function μ_x such that:

$$\mu_x = 1 \quad \begin{cases} if\ x \epsilon X \\ 0\ otherwise \end{cases} \tag{1}$$

A fuzzy set is shown by the formula 2.

$$\{x, \mu_{x'}, x \epsilon X\} \tag{2}$$

Where X is a variable taking its values in the reference space S, and x is a fuzzy subset of S, of membership

function $\mu_{\square}$. The process of fuzzy logic system is described throught five steps as described as follow.
The degrees of truth of such propositions are defined as values in [*0; 1*] from $\mu_{\square}$. All data sources are fuzzed into fuzzy membership functions. Fuzzy rules are created and take the form of IF THEN statement.
Fuzzy rules will be activated at each time t. The generated rules are combined in the rule base to be used in the calculation of the fuzzy output distribution.
The fuzzy output distribution is defuzzified to give a crisp output value.

VI. PROPOSED MODEL

We propose to conduct the TCP connection attack dataset by performing a binary classification. To do so, the large dataset was divided into several sub-datasets that will be trained and tested separately, and estimate the class of each TCP connection by different Artificial networks algorithm. Then, it is important to determine the positively and negatively correlated features because the algorithms we will use learn to predict the score of each feature instance from on the presence or absence of attack. Given results will be fuzzed by fuzzy logic Integral.
The sub-decision of ANN process is depicted in Figure 1 that will be merged with Fuzzy Integral Fusion to offer the best estimation of the optimal result. ANN_i is the sub-decision from different ANN_S ; W_i presents the m dimensional output vector $W_1^i, W_2^i \ldots W_n^i$ of the sub-data set i, where W_k^i presents the confidence of class k for a TCP connection sample decided by the sub-decision tree i. the fuzzy density of the sub-decision of $AN N_{ii}$ is presented by g_i

To evaluate this fuzzy logic as classifier algorithm, we use the following formal notation; Let $f_1, f_2 \ldots f_k$ be a predefined set of k features presented in network connection. Each feature f_i could be expressed in term of percentage of correct classification (PCC) given by each individual network sensor.
Let W_{i_r} be the function that calculate the feature F_i that occurs in the network connection n_c . Hence, every scenario of connection is presented by the following review vector.

$$W_{nc} = W_{nc1}, W_{nc2} \ldots W_{nc3} \quad (3)$$

In the proposed network attack detection process, we give to each network connection nc the class cl. We evaluate our fuzzy set classier by three steps; Fuzzification, logic rule's generation and Defuzzification.

A. Fuzzification

To calculate the membership values for each of the dataset input, each ANN sub-decision was ranged and the average value is estimated as normal, attack and suspicious connection that they are successfully noted by A (Attack), N (Normal) and S (suspicious). The calculated membership function was involved to define membership index related with each membership rate of the three attributes as shown in the following figure. The value of intrusion is partial.

C. Fuzzy Rules Generation

The rules were generated in the form of an IF THEN statement. All possible permutations were enumerated of the membership values of the three attributes. At first, all thirty permutations were used to generate the rules. However, it was difficult, for some permutation, to deduce the result which led to a low performance of the detection system. That is why, we choose to select only the permutations that led to a flexible way to infer the consequent of the rules and it reduced to only nine permutations. The permutations were calculated as the precedent for each rule generation. In the training data, we experiment the average value for each attribute in the normal, attack and merged data and concluded that for some attributes the average value degraded in the existence of attacks when it rose for some attributes. The result of each rule was dependant to the behavior of the average value of each attribute in the class of the connection. An example of the rules is offered below. We develop our network attack classier in JAVA using an open code source.

VII. EVALUATION RESULTS

In this part, we conduct the proposed fuzzy logic attack classifier, by which, we divide our data-set on three sub-datasets by j-48 algorithm (j-48 is a system that extracts significant patterns from data, and then to build decision tree.) to construct three sub-decision that are (ANN_1, ANN_2, ANN_3). Hence, the fuzzy logic algorithm is containing to create the final decision. The table IV shows real values of fuzzy densities of ANN_s sub- decisions with the corresponding for two experiments. In the experiment I, we calculate the fuzzy densities g , the degree of importance of each ANN sub-decision. Our aim is how good this sub-decision performed on training sub-dataset. In the experiment II, we assigned the fuzzy densities g is calculated as follows:

$$\frac{a_i}{\sum_{i=1}^{n} a_i} \quad (4)$$

Where i a is the classification accuracy of ANN_i sub-decision on the training sub-dataset i, and n is the number of sub-dataset. Table2 shows the experimental results. False positive rate (FPR) is the rate of normal data that the system falsely determines to be intrusive. False negative rate (FNR) is the rate of attack data that the system falsely determines to be normal. Error rate (ER) is the overall rate of misclassification test cases. According to the results shown in Table 2, we can conclude that:
The detection performance of ANN is not better than that of ANN_1 , ANN_2 and ANN_3 because of the over fitting in ANN decision learning. The FPR of ANN_1 is higher than

that of ANN because there are more Normal features belong to test dataset are not in training sub-dataset of ANN_1 comparing with other training sub-datasets. In the experiment I, the misclassification value of FLF_1 is lower than that of single sub-decision tree in FPR and ER (Error rate), but higher than that of single ANN sub-decision in FNR. Through adjusting fuzzy density, the results of experiment II present the misclassification rate of FLF_2 is lesser than that of single ANN sub-decision in FPR, FNR and ER. Evidently, the detection accuracy of FlF2 is higher than that of FLF_1.So, it is essential to select proper fuzzy density to improve detection performance. In addition, fuzzy logic fusion is better to single ANN sub-decision and a big decision tree in terms of classification performance for intrusion detection.

VIII. CONCLUSION

In this present paper, we offered a data fusion method for attack detection in network connection dataset using the fuzzy logic fusion (FLF) algorithm. We deduce that the approach of FLF results are better than evidence theory ones that we have proposed in [28, 29]. Especially, if we are dealing with great large dataset. Other gain of methodology is that the detection efficacy of FLF is better than a big ANN based decision on a large dataset. Another benefit of this methodology is that not only are the fusion results merged but that the importance of the each ANN sub-decision is also considered. The experimental results demonstrate that this technique is superior to the ANN based decision of mining on a large dataset and single ANN based sub-decision in terms of classification accuracy. Nevertheless, we could discuss on the issue of fizzing the ANN decision by some alternative fuzzy integral. As future work, we aim to concept the challenge of attack analysis in network connections as more than binary classification problem. In fact, it is possible to classify the attack in more than two classes like ”DOS”, ”BROB”, ”R2L”, etc.

II.

Furthermore, we plan to replace this problem as a regression problem where we can approximate the degree of affinity for the attack rather than a simple negative/positive class.

III.

As well as, we aim to involve more experiments on diverse type of random user-calculated data other than NSL-KDD

Our studies suggest that the issue of classifying attacks derived from different sources of different information cannot be solved in entirely supervised and unsupervised techniques. A data fusion technique gives a promising way for future research.

IV. REFERENCES

[1] T. Singleton, The Top 5 Cybercrimes, 1st ed. AICPA, 220 Leigh Farm Road, Durham: American Institute of CPAs, 2013.

[2] M. Gercke, Understanding cybercrime phenomina, challenges and lega response. ITU, 2012.

[3] M. Thottan, C. Ji, and F. House, “Anomaly detection in ip networks,” IEEE Transactions on Signal Processing, vol. 51, no. 8, pp. 2191–2204, 2003.

[4] S. Y. Shahul Kshirsagar, “Intrusion detection systems:a survey and analysis of classification techniques,” International Journal of Scientific Research Engineering and Technology IJRSET, vol. 3, no. 4, pp. 742– 747, 2014.

[5] S. M. V Jaiganesh and P. Sumathi, “Intrusion detection systems: A survey and analysis of classification techniques,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 4, pp. 1629–1635, 2013.

[6] T. Singleton, The Top 5 Cybercrimes, 1st ed. AICPA, 220 Leigh Farm Road, Durham: American Institute of CPAs, 2013.

[7] M. Gercke, Understanding cybercrime phenomina, challenges and lega response. ITU, 2012.

[8] M. Thottan, C. Ji, and F. House, “Anomaly detection in ip networks,” IEEE Transactions on Signal Processing, vol. 51, no. 8, pp. 2191–2204, 2003.

[9] S. Y. Shahul Kshirsagar, “Intrusion detection systems:a survey and analysis of classification techniques,” International Journal of Scientific Research Engineering and Technology IJRSET, vol. 3, no. 4, pp. 742– 747, 2014.

[10] S. M. V Jaiganesh and P. Sumathi, “Intrusion detection systems: A survey and analysis of classification techniques,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 4, pp. 1629–1635, 2013.

[11] J. K. Monowar Bhuyan, D.K. Bhattacharyya, “Network anomaly detec-tion: Methods, systems and tools,” EEE Communication Surveys and Tutorials, vol. 16, no. 1, pp. 303–336, 2014.

[12] A. Dallai, T. Omrani, B. Rhaimi Chibani, “Evidence Theory Data Fusion-Based Method for Cyber-Attack Detection”, in 4th International Conference on Advanced Technologies For Signal and Image Processing ATSIP 2018, March 21-24, 2018 , Sousse, Tunisia.

[13] G. A. Haidar and C. Boustany, “High perception intrusion detection system using neural networks,” 2015.

[14] T. Omrani, A. Dallai, B. Rhaimi Chibani, ”Fusion of ANN and SVM Classifiers for Network Attack Detection”, in 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA),374-377, 2017, Monastir, Tunisia.

[15] Statistical Data Mining Tutorials.

[16] elf-aware services: Using bayesian networks for detecting anomalies in Internet-based services, 2001.

[17] A. A. Imam Riadi, Jazi Eko, “Log analysis techniques using clustering in network forensics,” International Journal of Computer Science and Information Security(IJCSIS), vol. 10, no. 7, pp. 303–336, 2012.

[18] Y. Tsuruoka and J. Tsujii, “Training a naive bayes classifier via the em algorithm with a class distribution constraint,” CONLL ’03 Proceedings of the seventh conference on Natural language learning at HLT-NAACL, vol. 4, pp. 127–134, 2003.

[19] M. H. Mohamed Dewan, Farid Nouria and R. Zahidur, “combining naive bayes and decision tree for adaptive intrusion detection,” International Journal of Network Security and Its Applications (IJNSA), vol. 2, pp. 12–25, april 2010.

[20] N. Hurley, Z. Cheng, and M. Zhang, “Statistical attack detection,” in Proceedings of the Third ACM Conference on Recommender Systems, ser. RecSys ’09. New York, NY, USA: ACM, 2009, pp. 149–156.

[21] J. Lee, K. Cho, C. Lee, and S. Kim, “Voip-aware network attack detection based on statistics and behavior of sip traffic,” Peer-to-Peer Networking and Applications, vol. 8, no. 5, pp. 872–880, Sep 2015.

[22] L. A. Zadeh, “Soft computing and fuzzy logic,” IEEE Softw., vol. 11, no. 6, pp. 48–56, Nov. 1994.

[23] Y. Bai and D. Wang, Fundamentals of Fuzzy Logic Control — Fuzzy Sets, Fuzzy Rules and Defuzzifications. London: Springer London, 2006, pp. 17–36.

[24] E. Trillas and L. Eciolaza, Fuzzy Logic: An Introductory Course for Engineering Students. Springer Publishing Company, Incorporated, 2015.

[25] C. Liu, G. Qi, H. Wang, and Y. Yu, “Fuzzy reasoning over rdf data using owl vocabulary,” in Proceedings of the 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology - Volume 01, ser. WI-IAT ’11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 162–169.

[26] P. Dondio and L. Longo, “Computing trust as a form of presumptive reasoning,” in Proceedings of the 2014 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT) - Volume 02, ser. WI-IAT ’14, Washington, DC, USA, 2014, pp. 274–281.

[27] S. Liu, H. Yu, C. Miao, and A. C. Kot, "A fuzzy logic based reputation model against unfair ratings," in Proceedings of the 2013 International Conference on Autonomous Agents and Multi-agent Systems, ser. AA-MAS '13, Richland, SC, 2013, pp. 821–828.

[28] M. S. Fariba Haddadi, Sara Khanchi and V. Derhami, "Intrusion detection and attack classification using feed-forward neural network," in Second International Conference on Computer and Network Technology, 2010.

[29] A. B. V Chandola and V. K. V, "Anomaly detection: A survey," ACM Comput. Surv., pp. 15–58, 2009.