Introducing a Two-step Strategy Based on Deep Learning to Enhance the Accuracy of Intrusion Detection Systems in the Network

Ali Bahmani[1*], Amirhossein Monajemi[2]
1- Department of Computer, Islamic Azad University, Isfahan (Khorasgan) Branch, Isfahan, Iran.
Email: ali.bahmani@live.com (Corresponding author)
2- Department of Artificial Intelligence Engineering, University of Isfahan, Isfahan, Iran.
Email: monadjemi@eng.ui.ac.ir

Received: September 2018 Revised: October 2018 Accepted: December 2018

ABSTRACT:
Intrusion Detection System is one of the most important security features of modern computer networks that can detect network penetration through a series of functions. This system is independently used (e.g. Snort) or with various security equipment (such as Antivirus, UTM, etc.) on the network and detects an attack based on two techniques of abnormal detection and signature-based detection. Currently, most of the researches in the field of intrusion detection systems have been done based on abnormal behavior using a variety of methods including statistical techniques, Artificial Intelligence (AI), data mining, and machine learning. In this study, we can achieve an effective accuracy using a candidate class of the KDD dataset and deep learning techniques.

KEYWORDS Intrusion Detection System, Network Security, Deep Learning.

1. INTRODUCTION

With the development of information technology, security is recognized as a key role in the permanence of a modern organization. Today, several approaches and tools are used to provide IT security such as firewalls, antivirus, etc. [1]. Due to the increasing number of attacks and their complex nature, these tools may not be able to block the network penetration in some cases [2]. Therefore, using an intelligent mechanism such as Intrusion Detection System (IDS) can be effective in predicting the attacks and reducing the risks of the organization's security.

IDS is software or hardware that is used in the network and run through three functions of monitoring, detection, and response (in the form of alert, not action), facing an attack or infiltration [3]. In order to clarify the issues, it is necessary to clarify the IDS diagnostic methods, classification of IDS systems and different types of attacks.

1.1. Detection Methods in IDS Systems

1.1.1.Pattern-based methods

In this technique, an attack or penetration is discovered based on a predetermined pattern. In other words, the patterns associated with different attacks are already registered locally and the network traffic patterns are compared to those previously known and, if they are similar, it would be detected as an attack or infiltration. In this method, the detector usually has a database of signatures or attack patterns and tries to find similar patterns to those of its database by checking the network traffic and database updates are usually done by a specialist.

1.2.1.Abnormal behavior detection methods

This procedure demands distinguish between normal and abnormal behavior in the system and suggest a pattern for this, in which an abnormality may indicate a penetration. To create these patterns, techniques such as neural networks, machine learning, and safety systems can be used. Identifying normal behaviors and finding their patterns is necessary for detecting abnormal behavior. The behaviors that follow these patterns are normal, and events that are more or less common with these patterns are recognized as abnormal behavior. Unlike the first method, there is a chance of misdiagnosis if the system faces a new model [3].

1.2. Category of Known Attacks on the Network

According to Table 1, Attacks are categorized into four general categories as following:

- Type 1: Denial Of Service (DOS) attacks

The Attacker sends a large number of requests to the server and thus the server would be busy responding to unrealistic requests.

- Type 2: Probe attacks

It includes six types of attacks in which an application scans IP addresses and identifies vulnerabilities in the system. Once the vulnerability has been discovered, it can begin to collect information from the victim's system.

- Type 3: User to Root (U2R) attacks

The attacker pretends to be a legitimate user of the system and accesses the root of the system and uses vulnerabilities in the system without permission.

- Type 4: Remote to Local (R2L) attacks

An unauthorized attacker accesses the network through remote networks as a local user of the machine and exploits the vulnerabilities of the machine [4].

Table 1. Types of attacks known in KDD

DOS	Apache2, back, land, mailbomb, neptune, pod, proccesstable, smurf, teardrop, udpstorm
U2R	buffer_overflow, httptunnel, ps, loadmodule, Multihop, perl, rootkit, sqlattack, xterm
R2L	ftp_write, guess_password, imap, named, phf, sendmail, snmpgetattack, snmpguess, spy, warezclient, warezmaster, worm, xlock, xsnoop
Probe	ipsweep, mscan, nmap, portsweep, saint, satan

1.3. Use of Deep Learning in the Diagnostic Process

The deep learning process begins by training the layers of a neural network. A Convolutional neural network (CNN) consists of three main layers: convolution, pooling and fully connected layer. In each CNN, there are two stages for training. Feed-forward and backpropagation steps. In the first step, input content is entered into the network, which is the same as the multiplication of the point between the input and the parameters of each neuron. Then the network output is calculated. To set network parameters or network training, the output is used to calculate the network error rate. For this purpose, the network output is compared with the correct response using a loss function, and thus the error rate is calculated. After that, the backpropagation step begins based on the calculated error rate. In this step, each parameter is calculated according to the chain rule, and all parameters are changed according to the effect on the generated error in the network. After the parameters are updated, the feed-forward step will start again, and after completing the appropriate number of these stages, the network training will end [5].

Currently, AI-based penetration detection, data mining and machine learning are one of the most important issues that have been considered in designing these systems. Although a complete and comprehensive method for designing intrusion detection systems based on abnormal behavior has not yet been provided, techniques based on fuzzy neural networks and support vector machine (SVM) are among the most successful methods that have yielded significant results so far [4]. Considering the success of neural networks in the of intrusion detection, this study tries to use a two-stage method based on deep learning in order to provide an acceptable rate of accuracy.

2. LITERATURE REVIEW

The production, recording, and review of events date back to the late 1970s and early 1980s. This process includes recovery operations in the event of an error, restoration of system events, and abuse detection, by which it is possible to check the time and date of event, the user ID of the event creator (this ID should be unique to each user), the type of event or incident, and the success or failure of that event was determined.

Since 1980, three generations of intrusion detection systems have been introduced:

1- Host-based systems since 1980: These systems have been effective in gathering data at the operating system level and the concept of abnormalities and abuse was first used in these systems.

2- Network-based systems since 1990: These systems are used to collect data from network traffic, detect anomalies (extraction of normal traffic characteristics in the network), and malicious use (network attack detection and its impact on network efficiency).

3- Incomplete resource-based intrusion detection systems: These systems are designed to collect data from the host and network based on distributed architecture. With the advent of these systems, the need for automated methods for analyzing traffic has been increasingly considered, and techniques such as data mining, artificial intelligence, and machine learning in detecting abnormal traffic and intrusion detection have become the focus of expertise [6].

As it is presented in table 2, here are some examples of works done in this area:

- Lee et al. (1998), by analyzing user activities, programs, and operations performed on a computer system enabled the detection of abnormal behavior. Simple and fast implementation but low performance are features of this method are. It is one of the oldest processes that discovers the intrusion based on a non-systematic method and a series of events which are generated by computers and program [7].
- Kabiri et al. (2005) analyzed the network traffic, system-related events, and user behavior through the Bayesian method and statistical techniques. Identifying abnormal behavior and samples became

possible in this study. The characteristics of this method are the appropriate speed and efficiency [8].

- Ying Chung et al. (2012), detected the abnormal behavior at 93.3 accuracy rates using the congestion optimization method in selecting features and the method of optimizing particle swarm in classifying samples [9].
- Zbeel et al. (2013) used the genetic algorithm and the evolutionary learning method investigated the behavior of users and known examples of attacks [10].
- Horng et al. (2011) reviewed the network traffic samples using a support vector machine, which allows for the effective detection of known and unknown attacks with appropriate detection rates [11].
- Chen et al. (2016), could detect unknown attacks with appropriate detection rates using Markov's model in addition to analyzing network traffic and related events in the form of a multi-stage process [12].
- Ashfaq et al. (2017) used a fuzzy method to examine network traffic and records related to network behavior and provided detection of abnormal behavior with high detection rates [13].
- Dash (2017) used the neural network to examine network traffic and records associated with the behavior of the network, which allows the detection of abnormal behavior and known samples with a high degree of accuracy between 98.18 and 94.9 [14].
- Chen et al. (2016) analyzed the network traffic using the security systems approach, which allows the detection of abnormal events and known attacks with appropriate detection rates [15].

3. MATERIALS AND METHODS

In this study, KDD dataset was used which is considered to be the most important research reference in the field of network intrusion detection systems and is the result of a nine-week trial of TCP raw data in the Darpa lab. The 99 Cup KDD dataset contains 41 extracted attributes for each connection, which specifies each label in terms of the connection state that is normal or attacked. Identified attacks are divided into four categories according to the following table [16].

The next step is to select the appropriate features in order to optimize the learning rate in the deep learning technique. Nowadays, in the same research, all input data is used as inputs of the model, all of which do not have the same ability to predict classes. We suggest selecting different subsets of the features and use the deep learning technique to teach the model. To begin with, we start the deep learning technique using all the dataset features and calculate the accuracy level. Then using the greedy method, we evaluate the various subset to get an optimal response. We continue to use the new subset feature to repeat the deep learning process. The ultimate goal is to obtain an acceptable rate of accuracy. To perform the processes, we use the Rapidminer tool, the Optimize Selection operators or Brute Force (to select the random features collection), and the H2O Deep Learning (for the deep learning process).

Table 2. Comparison of methods used in intrusion detection systems. Discovered Methodology: AD: anomaly-based detection, SD: signature-base detection. Technology: H: host-based, N: network-based, K: Detectable Attacks: known attacks, U: unknown attacks, B: both known and unknown attacks. Efficiency: H: high, M: moderate, L: low

Methods	Detection Methodology		Technology	Detectable Attacks	Efficiency	Advantages and Disadvantages
	AD	SD				
Static Methods	*	*	H/N	B	M/L	Simple implementation but low accuracy
Bayesian Methods	*	*	N	B	H	Appropriate speed and accuracy
Support Vector Machine	*	*	N	B	H	False positives and high recognition rates
Markov Methods	*		H/N	U	M	Forecast and automatic learning
Neural Network	*	*	N	B	M/H	Automatic learning, error tolerance
Fuzzy Logic	*		H/N	U	H	Extensible and configurable, highly flexible
Genetic Algorithm		*	N	K	L	Use of evolutionary learning methods
Artificial Safety Systems	*	*	H	B	M	Expandable to a variety of models

Intelligent Swarm Optimization Method	*		N	U	H	Using Artificial Intelligence Techniques

3.1. Optimize Selection

This operator is used to identify the most relevant features based on greedy algorithms. The greedy algorithm applies a problem-solving method following a local optimal selection at each step, searching an absolute optimum. In some cases, a greedy strategy may not provide an optimal solution, but a greedy exploration may offer local optimal solutions that approximate an absolute optimal solution. Optimize selection uses Forward Selection and Backward Elimination algorithms for this purpose [17].

3.2. H_2O Deep Learning

This operator is used to implement the deep learning technique, in which a number of samples are entered as inputs to the network and the network output is calculated. Then, based on the results, the network error rate is calculated. Finally, based on the error rate of each step, the back-propagation operation begins. In this step, each parameter is calculated according to the chain rule, and all parameters are changed according to the effect on the generated error in the network. After the parameters are updated, the feed-forward is started again and ends after successive repetitions based on the optimal detection rate of the network training [18].

4. RESULTS AND DISCUSSION

In the first step, we began the deep learning process, whose results are presented in Table 3 based on the number of hidden layers. As can be seen, the accuracy level decreases by increasing the number of hidden layers from 10 layers to the top. Therefore, subsequent experiments will be repeated based on 10 layers. Using the optimize selection operator, features in Table 4 are considered as candidates. The modeling process is based on deep learning, with 4408589 samples and 10 layers.

Finally, all KDD dataset fields are removed except for the items in Table 4 and the deep learning process is performed with 10 hidden layers and the final accuracy is 99.55. As can be seen, the calculated accuracy value is 0.26, 0.2, and 0.24, less compared to tests No. 2, 6, and 10, respectively. This difference is small compared with other methods, and the total final accuracy rate shows a high value. Another important issue that was proven in this experiment is the dramatic reduction in memory usage and time to respond. Using this method, we were able to reduce the number of processed elements by about 50%, resulting in less usage of memory and system resources.

Table 1. Test results for deep learning actor and number of hidden layers.

Test No.	Number of hidden layers	Number of modeling samples	Accuracy
1	5	900001	99.26
2	10	900001	98.81
3	15	900001	99.27
4	20	900001	99.07
5	5	1800002	99.71
6	10	1800002	99.75
7	15	1800002	99.34
8	20	1800002	99.42
9	5	4408589	99.73
10	10	4408589	99.79
11	15	4408589	99.72
12	20	4408589	99.63

Table 2. Sub-Candidate.

No.	Feature
1	protocol_type
2	Flag
3	src_bytes
4	Land
5	wrong_fragment
6	num_failed_logins
7	logged_in
8	num_compromised
9	root_shell
10	num_root
11	num_file_creations
12	num_access_files
13	num_outbound_cmds
14	is_host_login
15	srv_rerror_rate
16	diff_srv_rate
17	dst_host_srv_count
18	dst_host_same_src_port_rate
19	dst_host_srv_diff_host_rate
20	dst_host_serror_rate

5. CONCLUSION

In this article, we first introduced different methods of detecting network intrusion and then presented different types of attacks and the researches which have been done related to the detection of abnormal traffic. Considering the history and accurate functioning of neural networks in the detection process, a special type of these networks was used as a deep learning network. Network was trained in two stages using training data from KDD and accuracy Recognition and resource usage were compared. In the first stage, the accuracy of detection was 99.55, and in the next step using greedy methods, a class of the candidate were defined. The detection accuracy based on these new features was slightly reduced, but the resource consumption decreased by 50% compared to the previous stage.

REFERENCES

[1] Rhodes-Ousley M. **"Information Security: the Complete Reference",** *McGraw Hill Education*; 2013.

[2] McClure S, Shah S, Shah S. **"Web Hacking: Attacks and Defense"**, *Addison-Wesley Longman Publishing* Co., Inc.; 2002.

[3] Liao H-J, Lin C-HR, Lin Y-C, Tung K-Y. **"Intrusion Detection System: A Comprehensive Review",** *Journal of Network and Computer Applications*. ; Vol. 36(1),16-24, 2013.

[4] Kumar V, Chauhan H, Panwar D. **"K-means Clustering Approach to Analyze NSL-KDD Intrusion Detection Dataset",** *International Journal of Soft*. 2013.

[5] LeCun Y, Bengio Y, Hinton G. **"Deep learning. Nature"**, pp. 521(7553):436, 2015.

[6] Kemmerer RA, Vigna G. **"Intrusion Detection: a Brief History and Overview",** *Computer.* ; Vol. 35(4):supl27-supl30, 2002.

[7] Lee W, Stolfo SJ, Mok KW, editors. **"Mining Audit Data to Build Intrusion Detection Models",** *KDD*; 1998.

[8] Kabiri P, Ghorbani AA. **"Research on Intrusion Detection and Response: A Survey",** *I. J Network Security*, Vol. 1(2), pp. 84-102, 2005.

[9] Chung YY, Wahid N. **"A hybrid network Intrusion Detection System Using Simplified Swarm Optimization (SSO)",** *Applied Soft Computing*., Vol. 12(9), pp. 3014-22, 2012.

[10] Zbeel BM. **"Using Genetic Algorithm for Network Intrusion Detection",** *kufa studies center Journal,* Vol. 1(29), pp. 209-24, 2013.

[11] Horng S-J, Su M-Y, Chen Y-H, Kao T-W, Chen R-J, Lai J-L, et al. **"A Novel Intrusion Detection System Based on Hierarchical Clustering and support Vector Machines",** *Expert systems with Applications*., Vol. 38(1), pp. 306-13, 2011.

[12] Chen C-M, Guan D-J, Huang Y-Z, Ou Y-H. "Anomaly network intrusion detection using hidden Markov model", *Int J Innov Comput Inform Control*, Vol. 12, pp. 569-80, 2016.

[13] Ashfaq RAR, Wang X-Z, Huang JZ, Abbas H, He Y-L. **"Fuzziness Based Semi-Supervised Learning Approach for Intrusion Detection System",** *Information Sciences*., Vol. 378, pp. 484-97, 2017.

[14] Dash T. **"A Study on Intrusion Detection using Neural Networks Trained with Evolutionary Algorithms",** *Soft Computing*., Vol. 21(10), pp. 2687-700, 2017.

[15] Chen M-H, Chang P-C, Wu J-L. **"A Population-Based Incremental Learning Approach with Artificial Immune System for Network Intrusion Detection",** *Engineering Applications of Artificial Intelligence*. Vol. 51, pp. 171-81, 2016.