Deep Learning in Intrusion Detection Systems

Conference Paper · December 2018

DOI: 10.1109/IBIGDELFT.2018.8625278

Gozde Karatas
T.C. Istanbul Kultur University
18 PUBLICATIONS **53** CITATIONS

Önder Demir
Marmara University
27 PUBLICATIONS **100** CITATIONS

Deep Learning in Intrusion Detection Systems

Gozde Karatas
Mathematics and Computer Sciences Dept.
Istanbul Kultur University
Istanbul, Turkey
g.karatas@iku.edu.tr

Onder Demir
Computer Engineering Department
Marmara University, Technology Faculty
Istanbul, Turkey
odemir@marmara.edu.tr

Ozgur Koray Sahingoz
Computer Engineering Department
Istanbul Kultur University
Istanbul, Turkey
sahingoz@gmail.com

***Abstract*—In recent years, due to the emergence of boundless communication paradigm and increased number of networked digital devices, there is a growing concern about cybersecurity which tries to preserve either the information or the communication technology of the system. Intruders discover new attack types day by day, therefore to prevent these attacks firstly they need to be identified correctly by the used intrusion detection systems (IDSs), and then proper responses should be given. IDSs, which play a very crucial role for the security of the network, consist of three main components: data collection, feature selection/conversion and decision engine. The last component directly affects the efficiency of the system and use of machine learning techniques is one of most promising research areas. Recently, deep learning has been emerged as a new approach which enables the use of Big Data with a low training time and high accuracy rate with its distinctive learning mechanism. Consequently, it has been started to use in IDS systems. In this paper, it is aimed to survey deep learning based intrusion detection system approach by making a comparative work of the literature and by giving the background knowledge either in deep learning algorithms or in intrusion detection systems.**

***Index Terms*—Intrusion detection; Deep Learning; Security; Big Data;**

I. Introduction

Nowadays, due to the extended use of Internet of Things (IoT) concepts, there are huge numbers of networked physical devices which not only consist of computers but also vehicles, digital devices, sensors etc [1] Due to this huge size of the network and uncontrolled/anonymous structure of the Internet, preserving both information and communication of the company has emerged as a challenging issue for researchers [2]. Although, most of the systems use the firewalls for this prevention, Intrusion detection systems (IDSs), which are accepted as the second line of defense, play a crucial role to increase the security level of the system. Attackers are continuously trying to find new ways to bypass the prevention mechanism of the systems. Therefore, IDSs become an inevitable component of security systems.

The evolution of intrusion detection systems is motivated by some important facts as:

- New networked systems are so complex and therefore they are very prone to errors and these errors can be exploited by the intruders/hackers.
- Current network systems have some critical security deficiencies which put them as a target for the attackers. Although there are some additional tools and works, which are trying to find and fix these deficiencies, closing all of them is not possible mostly.
- Although there exist some intrusion prevention systems, absolute prevention cannot be possible. As a result, IDS emerged as an excellent mechanism to catch and identify the intrusions. After this step, a prevention mechanism can be automatically updated.
- Most of the prevention mechanisms preserve the system from the outsider attackers. However, lots of the attacks are carried out by the authorized users in the company, who are hard to detect. This type of attacks can be more harmful.
- New attack types are developed to cross these prevention and detection mechanisms. Therefore, security solutions should be upgraded by using some learning or update mechanism in a dynamic structure.

In general, IDSs contain three main components as depicted in Figure 1.

- Firstly, there should be a data collection mechanism which tracing the network flows
- Then, these data need to be used to identify the features, and a feature vector needs to be created.
- Finally, with the use of this vector, a classification engine is executed, and the traced flow is identified either as normal or as an intrusion according to previous knowledge:

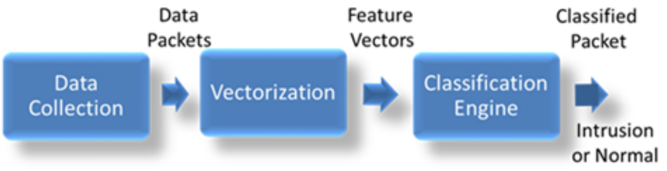

Fig. 1. Main Components of Intrusion Detection System

The critical part of an IDS system is the Classification Engine section which decides whether the converted feature vector fits the definition of an intrusion. Mainly this part can be either implemented as signature-based in which classifications are done according to previously defined signatures or anomaly based in which the normal packet flow of the system is learned by processing the previous data flows. Although the first one has a good decision time and reliability, It cannot detect the new attack types and therefore produce a low detection rate.

At the same time, the latter one has acceptable flexibility, robustness, and scalability. Therefore, for implementing a dynamic IDS system, mainly the anomaly detection techniques are preferred especially with a machine learning mechanism.

One of the important deficiencies of the machine learning based IDS mechanism is the need for huge training time for processing the big dataset of the previous data flow of the network. However, a newly emerged technology, named as deep learning, provides an effective learning mechanism by using some new approaches. With the simultaneously developed parallel solution technology, the training time is decreased, and the accuracy of the proposed systems are increased

In the literature, there are a few works about this topic which uses different deep learning approaches to detect the intrusions. In this paper, it is aimed to make survey research, which provides an overview of various aspects of deep learning-based intrusion detection system by giving the background knowledge about Deep Learning and Intrusion Detection topics. Additionally, we surveyed the current dataset which is used in the IDS implementation. At the same time, a comparative study is presented for depicting the differences between the implemented deep learning-based IDS systems

The rest of the paper is organized as follows. In the next section detailed information about Intrusion and Intrusion Detection System is given. In section 3, Machine learning and deep learning approaches are compared. Datasets which are especially preferred in IDS systems are listed, and some new datasets are explained in Section 4. The critical comparative work is presented in Section 5 which makes a comparative study on current literature on the topic. Finally, the paper is concluded with showing some directions for future works.

II. Intrusion and Intrusion Detection System

Intrusion: Cyber attack incidents are increasing with the increasing use of internet. Cyber attack is the virtual life of the bullying in normal life. In this attack person encounters such situations as harassment, threats and blackmail. The attack may be in the form of the capture of the persons' passwords or psychological pressure.

Intrusion Detection System: Intrusion Detection Systems are very important software or hardware security tools to remove threats that would otherwise occur when carrying information, to prevent unauthorized access or abuse, and to report attacks to those responsible for security [3]. Attack Detection was first introduced in Computer security threat monitoring and surveillance" survey published in 1980. The reasons for the need for intrusion detection systems;

1) It detects attacks that cannot be prevented by other security mechanisms.
2) It responds to the analysis phase before the attack occurs.
3) It allows attack analysis, system repair and the attacking factors to be corrected.

Advantages of intrusion detection systems early detection, detailed information collection, evidence quality. The weaknesses of the intrusion detection systems are as follows; packet fragmentation and timing attacks, mixing of scan sequence, package hijacking.

It is difficult to understand that packets arriving on the computer are sent for attack purposes. A packet arriving in the system may be sent for routine communication or an attack. Detecting an attack requires a difficult and intensive calculation.

Intrusion detection systems are classified according to several different criteria. IDSs can be classified; the architectural structure, the type of system it protects, and the processing time of the data. According to their location there are two types of intrusion detection systems, Host-Based and Network-Based [4]. Also IDSs can be classified according to their techniques; Signature-Based and Anomaly-Based.

- Host-Based IDS; server tries to detect attacks by listening to the traffic, registration files, and transactions.
- Network-Based IDS; listening to all the traffic directed to the network, recording the content of each data packet passing through the network, cutting off attacks when necessary and creating reports.
- Signature-Based IDS; is used to detect known attack types.
- Anomaly-Based IDS; is used to detect unseen attacks.

A. Intrusion Detection Approaches

In Intrusion Detection systems; techniques have been developed for modeling the data and create tables by classifying the modeled data [3]. The most used of these techniques are:

- Statistical: The first examples of systems are based on statistical measurements. Using these examples, a statistical model is created by examining user or system behavior. New intrusions are tried to be determined with the created statistical model. Some of the statistical methods used in intrusion detection are Principal Component Analysis, Chi-square distribution, Gaussian Mixture Distribution.
- Artificial Neural Networks; models the given data using graphs of artificial neurons. They associate their vectors with their own algorithms and create new data. It is an approach used to examine and learn the behavior of data in the system [5]. With a enhanced form of ANN some authors prefer the use of Deep Learning for its efficiency [6].
- Support Vector Machines; It is the most preferred method for intrusion detection systems. Used for selection of feature vector. Supper Vector Machines aims to distinguish between data from two classes in a most appropriate way with a feature vector. They used in many classification problems such as face recognition systems, sound analysis.
- Data Mining; it is known as reaching information among large-scale data. Used to extract rules by finding the relationship between data and users. Fuzzy Logic based on fuzzy set theory.
- Rule-Based Systems: It is developed by people who specialize in a specific area. These people examine the

system traffic and form rules and attack detection is done in this way.

- Fuzzy Logic: It is based on thinking like human beings and it is aimed to process them by converting them into mathematical functions.

III. Deep Learning

Deep learning is an improved machine learning technique for feature extraction, perception and learning of machines. Deep learning algorithms performs their operations using multiple consecutive layers. The layers are interlinked and each layer receives the output of the previous layer as input. It is a great advantage to use efficient algorithms for extracting hierarchical features that best represent data rather than manual features in deep learning methods [7], [8]. There are many application areas for Deep Learning, which covers such as Image Processing, Natural Language Processing, biomedical, Customer Relationship Management automation, Vehicle autonomous systems and others.

In Multilayer Architecture was firstly published in 1965 . In this study, the best features of the data were determined by statistical methods. Despite the developments made, Yann LeCun et al. developed the first successful Deep Neural Network application. They have done some examinations on the mailbox posts. After this work, Yann LeCunn again used a back-propagation algorithm to classify handwritten numbers using the ”LeNet” network.

In 1995, Brendan Frey, Peter Dayan and Geoffrey Hinton developed the Wake-Sleep Algorithm [9]. In this work, they show that it is possible to train a network containing hundreds of hidden layers, which 6 of them are completely connected and the study lasted two days.

A. Machine Learning vs Deep Learning

Experts in machine learning and deep learning have not yet reached consensus on these concepts. in this context, almost every day new ideas are being discussed. Machine Learning is an older concept than Deep Learning. Deep learning can also be called a technique that performs machine learning. The differences are listed below;

1) In deep learning, too much data is needed to bring the algorithm structure to the ideal.In machine learning, the problem can be solved with much less data because the person gives specific features to the algorithm.
2) Deep learning algorithms try to extract features from data. In machine learning, the features are determined by the expert.
3) While Deep Learning algorithms work on high performance machines, Machine Learning algorithms can work on ordinary CPUs.
4) In machine learning, the problem is usually divided into pieces, these parts are solved one by one and then the solutions are formed as a result of the solutions. In deep learning, the problem is solved end-to-end.
5) It takes a long time to train deep learning algorithms.

IV. Datasets

The most challenging phase to determine the performance of Intrusion Detection Systems is to find the appropriate data set. The information to be used for the data can be obtained by observing the network. Collecting information from the network is costly, therefore developers want to control their network or systems using available datasets. In this section, the most commonly used data sets for attack detection systems are mentioned.

A. KDD Cup99

It created by reason need for an appropriate data set for testing of intrusion detection systems. It was designed as a simulation data set in 1998. KDD Cup99 is especially used in the fields of data mining and machine learning. Mainly in standard data set of KDD Cup99, there are about 5 million data. About 80% of them are attack data. KDD Cup99 includes both training and test data. There are 41 features which can be categorized as basic features, traffic features, and content features, in the data set [4]. The data in this dataset can be classified into 5 main categories, 4 of them are attack, 1 is Normal.

- Normal; non-attack type data.
- Attack types: DOS (Denial of Service), Probe (Probing attacks), R2L (Root to Local) and U2R (User to Root).

The attacks are 22 types and each belongs to an attack category above. KDD Cup99 data contains numeric (in binary and real number format) and text information about categories of the request. Additionally, this data sets data also contains one additional feature in the end to show the label of the data whether it is an intrusion or not.

B. NSL-KDD

For the machine learning algorithms to work better on KDD Cup99, reduced data size by deleting duplicated records, and NSL-KDD dataset was created. It contains essential records of the complete KDD Cup99 dataset. It has the data features as the data content KDD Cup99 [10]. The NSL-KDD has the following differences over the original KDD Cup99;

1) The classifier does not give biased results because there are no redundant data in the training set.
2) The reduction ratio is lower because there is no repetitive data in the test set.
3) The number of records of selected records from each difficult level group is proportional to the percentage of records in the KDD dataset.

In each data there are 41 attributes unfolding different features of the flow and one label assigned to each either as an attack type or as normal. The 4 attack categories are further grouped as DOS, Probe, R2L and U2R.

C. CIC IDS 2017

This dataset created by The Canadian Institute for Cybersecurity (CIC). The CIC IDS 2017 dataset contains common attacks, which similar to the real-world data. It also includes the results of the network traffic analysis using CICFlowMeter, source, and destination IPs- ports, protocols and attack. Furthermore, the dataset is presumably available to anyone. CIC has identified eleven criteria that are necessary for building a reliable benchmark dataset [11]. These criteria are : Complete Network configuration, Complete Traffic, Labelled Dataset, Complete Interaction, Complete Capture, Available Protocols, Attack Diversity, Heterogeneity, Feature Set and Metadata.

The CICIDS2017 dataset consists of labeled network flows (including full packet payloads in .pcap format), the corresponding profiles and the labeled flows and CSV files for the machine and deep learning purpose.

D. CSE-CIC-IDS2018

The dataset created by The Canadian Institute for Cybersecurity (CIC) and Communications Security Establishment (CSE). It includes detailed information of attacks with abstract distribution models for computer systems. The dataset includes seven different attack scenarios such as Bruteforce attack, DoS attack, Web attack, Infiltration attack, Botnet attack, DDoS attack, and Heartleech [12];

- Bruteforce attack; They used FTP Patator and SSH Patator tools to collect these type of attacks.
- DoS attack; They used Hulk, GoldenEye, Slowloris and Slowhttptest tools to collect these type of attacks.
- Web attack; They used Damn Vulnerable Web App (DVWA) and In-house selenium framework (XSS and Brute-force) tools to collect these type of attacks.
- Infiltration attack; They used Nmap and portscan tools to collect these type of attacks.
- Botnet attack; They used screenshots and keylogging
- DDoS attack; They used Low Orbit Ion Canon (LOIC) for UDP, TCP, or HTTP requests.
- Heartleech; It is a DoS attack.

The CIC team recorded the raw data each day including the network traffic and event logs. In features extraction process from the raw data, they used the CICFlowMeter-V3 and extracted more than 80 network traffic features. Finally, they saved them as a CSV file per machine.

E. MCFP Bot Traffic Merged with Benign

Complete traffic traces of bot malware is provided by the Malware Capture Facility Project (MCFP). It developed in lab environment. This data set holds data on real bot infection to simulate an incident. Since individual bot malware examples are run and traffic traces are provided without benign traffic, labels can be efficiently applied to each event before merging. However, the absence of benign activity and the absence of false warnings as a result is a challenge to the power of representation of the data.For more detailed information about this dataset, [13] can be examined.

V. CONCLUSION

For preventing attacks to the networks, an intrusion detection system plays a very critical role in the cybersecurity domain. Its effectiveness directly depends on the used decision engine. To increase the flexibility of the system, instead of signature-based detection, it is required to implement the system as anomaly detection with a learning system. One of the newest training and classification technique, which is executed in this engine, is emerged as deep learning. Therefore, in this paper, it is aimed to provide a short survey of deep learning-based intrusion detection systems with the overview of various aspects of intrusion detection and deep learning algorithms. Additionally, this work lists and gives details about some publicly available datasets with their characteristics and shortcomings. We believe that this comprehensive survey on deep learning-based IDS could be helpful or researchers in this area. Although most of the researches proposed their system with the older dataset, as future work, it will be helpful to use the newest datasets with alternative deep learning approaches.

REFERENCES

[1] A. H. Ngu, M. Gutierrez, V. Metsis, S. Nepal, and Q. Z. Sheng, "Iot middleware: A survey on issues and enabling technologies," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 1–20, Feb 2017.

[2] W. Fu, X. Xin, P. Guo, and Z. Zhou, "A practical intrusion detection system for internet of vehicles," *China Communications*, vol. 13, no. 10, pp. 263–275, Oct 2016.

[3] G. Karataş, "Genetic algorithm for intrusion detection system," in *Signal Processing and Communication Application Conference (SIU), 2016 24th.* IEEE, 2016, pp. 1341–1344.

[4] G. Karatas and O. K. Sahingoz, "Neural network based intrusion detection systems with different training functions," in *Digital Forensic and Security (ISDFS), 2018 6th International Symposium on.* IEEE, 2018, pp. 1–6.

[5] O. Can and O. K. Sahingoz, "An intrusion detection system based on neural network," in *2015 23nd Signal Processing and Communications Applications Conference (SIU)*, May 2015, pp. 2302–2305.

[6] U. Cekmez, Z. Erdem, A. G. Yavuz, O. K. Sahingoz, and A. Buldu, "Network anomaly detection with deep learning," in *2018 26th Signal Processing and Communications Applications Conference (SIU)*, May 2018, pp. 1–4.

[7] B. Dong and X. Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in *Proc. IEEE ICCSN*, 2016, pp. 581–585.

[8] G. Zhao, C. Zhang, and L. Zheng, "Intrusion detection using deep belief network and probabilistic neural network," in *Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International Conference on*, vol. 1. IEEE, 2017, pp. 639–642.

[9] G. E. Hinton, P. Dayan, B. J. Frey, and R. M. Neal, "The" wake-sleep" algorithm for unsupervised neural networks," *Science*, vol. 268, no. 5214, pp. 1158–1161, 1995.

[10] G. Meena and R. R. Choudhary, "A review paper on ids classification using kdd 99 and nsl kdd dataset in weka," in *Computer, Communications and Electronics (Comptelix), 2017 International Conference on.* IEEE, 2017, pp. 553–558.

[11] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization." in *ICISSP*, 2018, pp. 108–116.

[12] T. Shibahara, T. Yagi, M. Akiyama, D. Chiba, and T. Yada, "Efficient dynamic malware analysis based on network behavior using deep learning," in *Global Communications Conference (GLOBECOM), 2016 IEEE.* IEEE, 2016, pp. 1–7.

[13] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *computers & security*, vol. 45, pp. 100–123, 2014.