School of Computer Science and Engineering

J Component report

Programme : B.Tech CSE with Spl. in AI and ML

Course Title : Information Security Management

Course Code : CSE3502

Slot : A2

Title: DoS Classification Using Deep Learning Techniques

Team Members: Sila Shivanandan (19BAI1141)

Ashwin U Iyer (19BAI1118)

Hitesh Goyal (19BAI1129)

Faculty: Dr. Ganapathy S.

Abstract

DoS attacks are the most destructive attacks that disrupt the secure operation of essential services provided by different organizations in the Internet community. DOS stands for denial of service attacks. These attacks are becoming increasingly complex and are expected to increase in number day by day, making it difficult to detect and counter these threats. It is necessary to identify and recognize abnormal behavior of Internet traffic. In this article, the process is supported by the latest data set containing the current form of DoS attacks. Our project combines well-known Deep Learning methods such as CNN, LSTM, CNN-LSTM, and DNN.

Keywords: DoS, AI, CNN, LSTM, DNN

Introduction

Many types of network attacks accompany the expansion of computer networks, especially the Internet. An international ransomware virus called Wannacry recently disrupted internet services in around 156 countries. According to Kaspersky Lab's fourth-quarter results, botnet-assisted attacks targeted assets in nearly 69 countries. The last quarter also saw the largest DoS-based botnet attack which lasted around 15.5 days and 371 hours. Crackers or dark hackers are constantly creating new forms of multi-layered DoS attacks that mostly occur at an OSI network and application layer. spoofed IP addresses to confuse source detection and carry out a large-scale attack. These attacks are quite huge, as the attack traffic consumes the network spectrum at the peak, thus reducing the legal packets. Ironically, the victims are government entities, finance companies, defense forces, and military agencies. Famous sites such as Facebook, Twitter, WikiLeaks, etc, had become victims of DoS that also observed interruptions in routine maintenance resulting in financial failures, depletion of service, and lack of access.

Our project deals with different AI methods such as CNN, LSTM, CNN-LSTM, and DNN for the detection and analysis of different forms of these attacks, including Smurf, UDP flood, and HTTP. This work was carried out.

2. Literature Survey

2.1 *A Deep Learning-based HTTP slow DoS classification approach using Flow Data, Muraleedharan N., Janet B. Centre for Development of Advanced Computing (C-DAC), Bangalore, India Computer Applications Department, NIT Tiruchirappalli, India.*
Received 28 February 2020; received in revised form 25 July 2020; accepted 23 August 2020
The popularity of the Internet introduces many network-enabled services that can be accessed by the user. But the adversaries are trying to deny these critical services to the user through Denial of Service (DoS) attacks. Presently, dealing with a DoS attack that targets the application layer using a slow traffic rate is one of the key challenges faced by the service providers. In this paper, a deep classification model using flow data is proposed to detect slow DoS attacks on HTTP. The classifier is evaluated using the CICIDS2017 dataset. The results obtained show that the classifier can obtain 99.61% accuracy.

2.2 *A Classification Framework to Detect DoS Attacks Ahmed Iqbal, Shabib Aftab, Israr Ullah, Muhammad Anwaar Saeed, Arif Husen Department of Computer Science, Virtual University of Pakistan.*
Received: 10 July 2019; Accepted: 22 July 2019; Published: 08 September 2019
The exponent increase in the use of online information systems triggered the demand for secure networks so that any intrusion can be detected and aborted. Intrusion detection is considered one of the emerging research areas nowadays. This paper presents a machine learning-based classification framework to detect Denial of Service (DoS) attacks.

2.3 *Data Mining Techniques in DoS/DDoS Attack Detection: A Literature Review Bayu Adhi Tama, Kyung-Hyune Rhee Department of IT Convergence and Application Engineering, Pukyong National University Busan 48513, South Korea*
This paper attempts to classify papers concerning DoS/DDoS attack detection using data mining techniques. Thirty-five papers were selected and carefully reviewed by authors from two online journal databases. Each selected paper was classified based on the function of data mining such as association, classification, clustering, and hybrid methods. The findings of this work indicate that classification and hybrid techniques received a great deal of attention from researchers. Our literature review provides a state of the art analysis concerning DoS/DDoS attack detection using data mining techniques.

2.4 *DOS ATTACKS AND DEFENSE MECHANISMS: A CLASSIFICATION Christos Douligeris and Aikaterini Mitrokotsa Department of Informatics University of Piraeus, Piraeus, Greece*

Denial-of-service (DOS) attacks pose an enormous threat to websites and are one of the most serious security problems on the Internet today. Because of their potential impact, Distributed Denial of Service (DDoS) attacks are of particular concern. With little or no warning, a DDoS attack can exhaust its victim's computing and communications resources in a short period of time. This article presents the problem of DDoS attacks and develops a classification of DDoS defense systems. Important characteristics of each category of attack and defense systems are described, and the advantages and disadvantages of each proposed scheme are described. The aim of the Document is to classify the existing attack and defense mechanisms in such a way that a better understanding of DDoS attacks can be achieved and more efficient defense mechanisms and techniques can be designed.

2.5 *DDoS attacks and defense mechanisms: classification and state-of-the-art Christos Douligeris, Aikaterini Mitrokotsa Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, Piraeus 18534, Greece Received 9 October 2003; accepted 13 October 2003*

Denial of Service (DoS) attacks are one of the biggest threats and one of the most serious security problems on the Internet today. Of particular concern are DDoS (Distributed Denial of Service) attacks, the impact of which can be correspondingly severe. With little or no warning, a DDoS attack can exhaust its victim's computing and communications resources in a short period of time. Due to the severity of the problem, many defense mechanisms have been proposed to combat these attacks. This document presents a structural approach to the DDoS problem by developing a classification of DDoS attacks and DDoS mitigation mechanisms. In addition, important characteristics of each category of attack and defense systems are described, and the advantages and disadvantages of each proposed scheme are described. The aim of the article is to classify the existing attack and defense mechanisms in such a way that a better understanding of DDoS attacks can be achieved and, as a result, more efficient and effective algorithms, techniques, and procedures can be developed to combat these attacks.

2.6 *A Survey on Latest DoS Attacks: Classification and Defense Mechanisms Rajkumar, ManishaJitendra Nene2 Department of Computer Engineering, Defense Institute Of Advanced Technology, Pune, India*

Distributed Denial of Service (DDoS) is defined as an attack in which multiple compromised systems attack a single target to make services unavailable to legitimate

users. It is an attack aimed at rendering a computer or network unable to provide normal services. DDoS attacks use many compromised intermediate systems called botnets that are remotely controlled by an attacker to launch these attacks. The DDOS attack basically results in a situation where an
entity cannot perform an action for which it is authenticated. This usually means that a legitimate node on the network cannot communicate with another node, or its performance is degrading. The sheer number of outages and outages caused by DDoS really pose an immense threat to the entire internet world today. Any commitment to computing, communication, and server resources such as sockets, CPU, memory, disk/database bandwidth, I/O bandwidth, router processing, etc. For a collaborative environment, this would certainly put the entire application at risk. It is necessary for researchers and developers to understand the behavior of the DDoS attack as it affects the target network with little or no warning. Therefore, the development of advanced intrusion detection and prevention systems to prevent, detect and respond to DDOS attacks is a critical necessity for cyberspace. Our rigorous survey study presented in this whitepaper outlines a platform to study the evolution of DDoS attacks and their defenses.

2.7 *A survey on DoS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools, and datasets*

Bushra Alhijawia, Sufyan Almajalia, Hany Elgalab, Haythem Bany, Salamehcd Moussa Ayyashe

Software-Defined Networking (SDN) is a modern networking approach that replaces traditional network architecture with a flexible architecture by separating the control plane from the data plane. SDN simplifies network management and monitoring through logically centralized intelligence, programmability, and abstraction. SDN architectures are vulnerable to attacks such as Denial of Service (DoS) attacks. This article evaluates and ranks research efforts on SDN and DoS. We classify research efforts into two groups: solutions to deal with DoS attacks on SDN and SDN-based solutions to deal with DoS attacks on networks. The first group of solutions includes six categories: TableEntry, Scheduling, Architectural, Flow Statistics, Machine Learning, and Hybrid solutions. Additionally, the article examines the tools and datasets considered by the reviewed posts. The article presents a detailed comparison between the examined approaches in terms of network devices, network layers involved, DoS attack types, and attack targets.

2.8 *Denial of service attacks: An overview*

Vinko Zlomislić; Krešimir Fertalj; Vlado Sruk

Denial of Service (DoS) attacks represent one of the most important threats to ensuring reliable and secure information systems. The rapid development of new and increasingly sophisticated attacks requires ingenuity to design and implement reliable

countermeasures. This article provides an overview of current DoS attack and defense concepts from a theoretical and practical perspective. Taking into account the worked-out DoS mechanisms, main directions for future investigations needed to defend against the evolving threat are suggested.

2.9 *Denial of Service Attack and Classification Techniques for Attack Detection Prajakta Solankar, Prof. Subhash Pingale, Prof. Ranjeetsingh Parihar Dept. Of Computer Science & Engineering, Solapur University SKN Sinhgad College of Engineering Pandharpur, Maharashtra, India*

The denial of service attack is a critical threat to the internet and it affects computer systems like web servers, database servers, etc. An internet user performs activities like email, online banking, news, general browsing, etc. A denial of service attack Attack (DoS) prevents the user from accessing these services. The main goal of attackers when performing a Denial of Service attack is to prevent legitimate users from using system resources. Because of this, DoS attacks must be detected. In this thesis, different techniques for classifying attacks are shown. KNearest Neighbor (KNN), Support Vector Machine (SVM), Decision Tree and Naïve Bayes are described and experimental results are obtained with weak tools.

2.10 *A Novel Approach for Classification and Detection of DOS Attacks Poonam Jagannath Shinde; Madhumita Chatterjee*

Recently, the use of the Internet and its users is increasing at a tremendous rate. During this growth, a well-protected network is the main requirement for all organizations. To secure a network, we need to protect it from attackers. Websites are a prime target for these attackers. Among all website attacks, one of the biggest threats to network functionality is the denial of service (DOS) attacks.DOS attacks exhaust the network resources of a specific Internet system or service, causing legitimate users to lose access to the resource. The DOS attack is an attacker's attempt to deny the user service. It is an attack that floods the targeted system with traffic that sends malicious information that can crash the system. In our approach, we use Support Vector Machine and C4.5 supervised learning algorithms on the NSL_KDD dataset for the effective classification of DOS attacks. We use a sniffer to monitor network IP packets and detect malicious and normal packets from traffic. Therefore, the results of the classifier are evaluated and the best result is displayed.

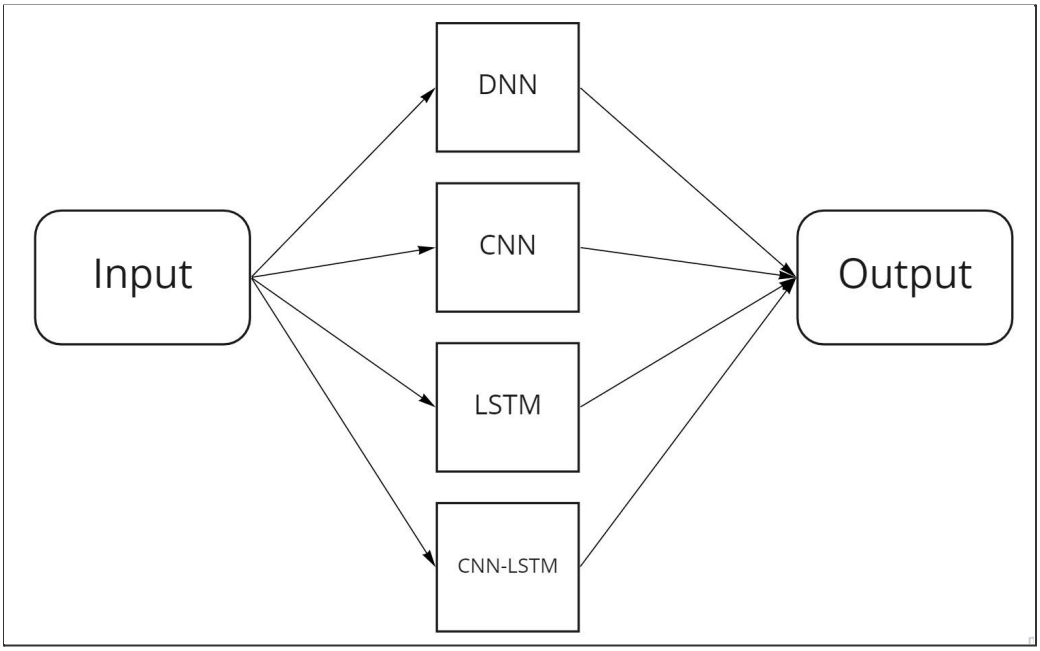
3. Proposed Model

3.1 Dataset

The KDD training dataset consists of approximately 4,900,000 single connection vectors each of which contains 41 features and is labeled as either normal or an attack, with exactly one specific attack type. The simulated attacks fall into one of the following four categories:

1. Denial of Service Attack (DoS): is an attack in which the attacker makes some computing or memory resource too busy or too full to handle legitimate requests, or denies legitimate users access to a machine.
2. User to Root Attack (U2R): is a class of exploit in which the attacker starts with access to a normal user account on the system (perhaps gained by sniffing passwords, a dictionary attack, or social engineering) and can exploit some vulnerability to gain root access to the system.
3. Remote to Local Attack (R2L): occurs when an attacker who can send packets to a machine over a network but who does not have an account on that machine exploits some vulnerability to gain local access as a user of that machine.
4. Probing Attack: is an attempt to gather information about a network of computers for the apparent purpose of circumventing its security controls.

3.2 Models



This is the basic structure of our Algorithms.

3.2.1 Original Model Architectures

CNN:

Optimizer was SGD, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 1 Dimensional Convolution Layer with 8 units of 1 kernel each (ReLU activation)
3. Max Pool of size 2
4. 1 Dimensional Convolution Layer with 5 units of 3 kernels each (ReLU activation)
5. Max Pool of size 2
6. Flattening with Dropout 0.5
7. 50 node Dense layer (ReLU activation)
8. Output layer with Softmax

LSTM:

Optimizer was Adam, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 5 Unit LSTM (ReLU activation)
3. Output layer with Softmax

CNN-LSTM:

Optimizer was Adam, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 1 Dimensional Convolution Layer with 2 units of 5 kernels each (ReLU activation)
3. Max Pool of size 1
4. 1 Unit LSTM with Dropout 0.1 (TanH activation)
5. Output layer with Softmax

DNN:

Optimizer was SGD, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 10 node Dense layer (ReLU activation) with Dropout 0.5
3. Output layer with Softmax

3.2.2 New Model Architectures

CNN:

Optimizer was SGD, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 1 Dimensional Convolution Layer with 8 units of 1 kernel each (TanH activation)
3. Max Pool of size 2
4. 1 Dimensional Convolution Layer with 5 units of 3 kernels each (TanH activation)
5. Max Pool of size 2
6. Flattening with Dropout 0.5
7. 50 node Dense layer (ReLU activation)
8. Output layer with Softmax

LSTM:

Optimizer was Adam, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 5 Unit LSTM (TanH activation)
3. Output layer with Softmax

CNN-LSTM:

Optimizer was Adam, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 1 Dimensional Convolution Layer with 2 units of 5 kernels each (TanH activation)
3. Max Pool of size 1
4. 1 Unit LSTM with Dropout 0.1 (TanH activation)
5. Output layer with Softmax

DNN:

Optimizer was SGD, and loss was categorical cross entropy. The model looked like below:

1. Input Layer
2. 10 node Dense layer (TanH activation) with Dropout 0.5
3. Output layer with Softmax

4. Results

DNN

Folds	**TanH**				**ReLU**			
	Precision	Recall	F1 Score	Accuracy	Precision	Recall	F1 Score	Accuracy
Fold 1	0.98	0.99	0.98	0.9891	0.98	0.99	0.98	0.9887
Fold 2	0.98	0.99	0.98	0.9890	0.98	0.99	0.98	0.9886
Fold 3	0.98	0.99	0.98	0.9890	0.98	0.99	0.98	0.9886
Fold 4	0.98	0.99	0.98	0.9890	0.98	0.99	0.98	0.9886
Fold 5	0.98	0.99	0.98	0.9890	0.98	0.99	0.98	0.9886

CNN

Folds	**TanH**				**ReLU**			
	Precision	Recall	F1 Score	Accuracy	Precision	Recall	F1 Score	Accuracy
Fold 1	0.99	0.99	0.99	0.9921	0.99	0.99	0.99	0.9899
Fold 2	0.99	0.99	0.99	0.9920	0.99	0.99	0.99	0.9897
Fold 3	0.99	0.99	0.99	0.9921	0.99	0.99	0.99	0.9897
Fold 4	0.99	0.99	0.99	0.9921	0.99	0.99	0.99	0.9898
Fold 5	0.99	0.99	0.99	0.9922	0.99	0.99	0.99	0.9898

LSTM

Folds	**TanH**				**ReLU**			
	Precision	Recall	F1 Score	Accuracy	Precision	Recall	F1 Score	Accuracy
Fold 1	0.98	0.99	0.98	0.9870	0.97	0.98	0.97	0.9790
Fold 2	0.98	0.99	0.98	0.9870	0.97	0.98	0.97	0.9788
Fold 3	0.98	0.99	0.98	0.9868	0.97	0.98	0.97	0.9787
Fold 4	0.98	0.99	0.98	0.9870	0.97	0.98	0.97	0.9789
Fold 5	0.98	0.99	0.98	0.9869	0.97	0.98	0.97	0.9787

CNN-LSTM

Folds	**TanH**				**ReLU**			
	Precision	Recall	F1 Score	Accuracy	Precision	Recall	F1 Score	Accuracy
Fold 1	0.98	0.99	0.98	0.9850	0.90	0.88	0.87	0.8832
Fold 2	0.98	0.98	0.98	0.9848	0.90	0.88	0.87	0.8831
Fold 3	0.98	0.98	0.98	0.9849	0.90	0.88	0.87	0.8830
Fold 4	0.98	0.99	0.98	0.9850	0.90	0.88	0.87	0.8833
Fold 5	0.98	0.99	0.98	0.9850	0.90	0.88	0.87	0.8833

We see that TanH activated CNNs perform best. The results displayed show that there is a very marginal increase in accuracy when we use TanH in place of ReLU. However, the CNN-LSTM results show conclusively that TanH activation is more effective than ReLU. These results have been tested by training the models multiple times and by getting similar results for conclusive results.

5. Conclusion

Based on the literature survey, it was observed that attempts to solve the problem of DoS classification involved using Machine Learning-based approaches, such as Naive Bayes [Salunkhe et al., 2015]. But Deep Learning architectures such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have shown promise in helping to identify DoS attacks, offering a robust and much more effective way of tackling the problem. This has been verified experimentally on the famous KDD-19 dataset. The feature extraction ability of CNNs based on the input is useful in identifying the relevant features of a packet. Similarly, LSTM and RNN-based architectures are extremely good at decoding long-term dependencies, which is another asset when it comes to the classification of DoS attacks. Thus, based on experimental data, we have been able to verify that using these models for DoS classification is a viable, effective and efficient approach.

Links

Code: https://github.com/indianeagle4599/DoS-Classification
Video: https://drive.google.com/file/d/1cXv-Ka-lug6H19wrzbVXTFujdY7SW7aw/view?usp=sharing

6. References

1. M. Alkasassbeh, G. Al-Naymat et.al," Detecting Distributed Denial of Service Attacks Using Data Mining Technique," (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, pp. 436-445, 2016. Science and Information Technologies, Vol. 6 (2), pp. 1096-1099, 2015.
2. Hoda Waguih, "A Data Mining Approach for the Detection of Denial of Service Attack", International Journal of Artificial Intelligence, vol. 2 pp. 99106(2013).
3. Dewan Md. Farid, Nouria Harbi, Emna Bahri, Mohammad Zahid ur Rahman, Chowdhury Mofizur Rahman," Attacks Classification in Adaptive Intrusion Detection using Decision Tree "International Journal of Computer, Electrical, Automation, Control, and Information Engineering, Vol:4, No:3, 2010.
4. Singh, S.K., Gupta, A.K. Application of support vector regression in predicting thickness strains in hydro-mechanical deep drawing and comparison with ANN and FEM (2010) CIRP Journal of Manufacturing Science and Technology, 3 (1), pp. 66-72.
5. Ramesh. G, Madhavi, K. "Summarizing Product Reviews using NLP based Text Summarization", International Journal of Scientific & Technology Research, September 2019. (Scopus).
6. Mangesh Salunke, RuhiKabra, Ashish Kumar." Layered architecture for DoS attack detection system by combine approach of Naive Bayes and Improved K Means Clustering Algorithm", International Research Journal of Engineering and Technology (IRJET), Volume: 02 Issue: 03, June-2015.
7. Ramesh G, Madhavi K., "Best keyword set recommendations for building service-based systems" International Journal of Scientific and Technology Research, October 2019.
8. T. Subbulakshmi et.al, "A Unified Approach for Detection and Prevention of DDoS Attacks Using Enhanced Support Vector Machine and Filtering Mechanisms", ICTACT Journal on Communication Technology, June 2013.
9. Yogeswara Reddy B, Srinivas Rao J, Suresh Kumar T, Nagarjuna A, International Journal of Innovative Technology and Exploring Engineering, Vol.8, No. 11, 2019, pp: 1194-1198.