Network Attack Detection Based on Neural Network LSTM

Zichao Sun[1,a], Peilin Lyu[2,b]

[1]Information and Communication, Communication University of China, Beijing, China

[2]Jilin University, Jilin, China

[a]sunzichao1014@163.com, [b]18770709@qq.com

Keywords: recurrent neural network, network attacks, hyperparameter, training model

Abstract: With the development of the times, the network security problem is becoming more and more serious, and the form of network attack is more complex and diverse. It can effectively detect various network attacks becomes the basis for effective prevention of network attacks. In recent years, artificial intelligence has attracted more and more people's attention, and its good learning ability has been favored by people. This paper uses the LSTM neural network with long and short memory function to train the KDD99 dataset, and identify the DOS according to the trained model. This is a research process of the planned adjustment for the hyperparameters to find the optimal solution after processing the data.

1. Introduction

A modern term for a network attack refers to an attack on the hardware, software, and data in the network system using vulnerabilities and security flaws in the network. With the rapid development of computers and the Internet in recent years, the network has shown a new development trend. Mainly reflected in the following six points:

- Increased automation and attack speed
- Attack tools are becoming more and more complex
- Finding security vulnerabilities is getting faster
- Firewall penetration is getting higher and higher
- Threats are becoming more and more asymmetric
- The threat to infrastructure will grow

A denial of service attack exploits multiple systems to attack one or more victim systems, causing the compromised system to refuse to provide services to its legitimate users. The degree of automation of the attack tool allows an attacker to install their tools and control tens of thousands of compromised systems to launch attacks. Intruders often search for address blocks that are known to contain a large number of vulnerable systems with high-speed connections, and cable modems, DSLs, and university address blocks are increasingly becoming targets for intruders planning to install attack tools. Because the Internet is made up of limited and consumable resources, and the security of the Internet is highly interdependent, denial of service attacks are very effective. A worm is a self-propagating malicious code. Unlike viruses that require users to do something to continue to breed, worms can multiply themselves. In addition, they can take advantage of a large number of security vulnerabilities, which can cause a large number of systems to be attacked within a few hours. Some worms include built-in denial of service attack payloads or Web site damage payloads, while others have dynamic configuration capabilities. However, the biggest influence of these worms is that because they generate a large number of scanned transport streams when they are transmitted, their propagation actually generates a denial of attack on the Internet, causing a large amount of indirect damage (such examples include: DSL routers; It is not caused by the scanning itself, but the scan-induced infrastructure network management (ARP) transport stream surge caused by the cable modem's ISP network is fully overloaded).

Therefore, it is possible to quickly and accurately detect that network attacks become an

important means of blocking network attacks. Nowadays, with the rapid development of artificial intelligence, artificial intelligence has gradually appeared in various fields of life. As an important member of artificial intelligence, neural network has excellent performance in the fields of image recognition and intelligent robots. Therefore, neural network technology is introduced in the field of network attack detection, and the model is trained according to the collected data to achieve the purpose of detecting network attacks quickly and accurately.

DoS attack refers to the flaw of intentional attack network protocol implementation or cruelly exhausting the resources of the attacked object through brutal means. The purpose is to prevent the target computer or network from providing normal service or resource access, so that the target system service system stops responding. It even crashes, and does not include intrusion into the target server or target network device in this attack. These service resources include network bandwidth, file system space capacity, open processes, or allowed connections. This type of attack can lead to a lack of resources. No matter how fast the computer is processed, how much memory capacity is, and how fast the network bandwidth is, the consequences of such an attack cannot be avoided.

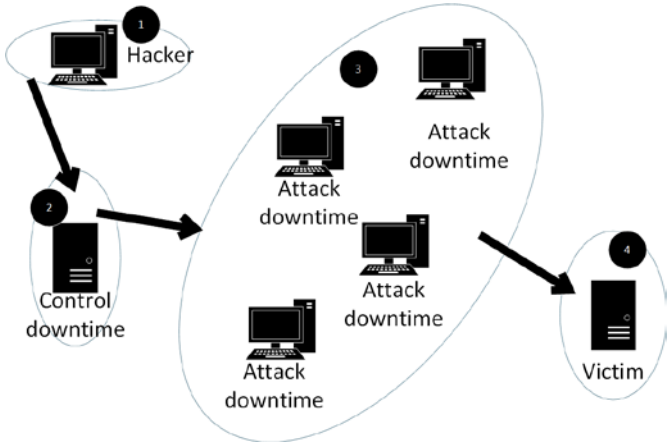

Fig.1 DOS Attack Diagram

2. LSTM

The most efficient sequence model in practical applications is called gated RNN, including networks based on long and short memories and gated loop units. The "permeation unit" integrates signals using different time constants and removes some of the connections used to model fine-grained time scales. Like the infiltration unit, the gated RNN idea is also based on the path that generates the transit time, where the derivative neither disappears nor explodes. The infiltration unit achieves this by manually selecting constant connection weights or parameterized connection weights. The gated RNN promotes it as a connection weight that can change at each time step. The infiltration unit allows the network to accumulate information for a longer duration, however, once the information is used, it may be useful to have the neural network forget the old state. We need the neural network to learn to decide when to clear the state, rather than making a manual decision.

Introducing the ingenious conception of self-loop to generate a gradient for a long-term continuous flow path is the core contribution of the initial length of the memory model. One of the key extensions is to make the right of self-looping context-sensitive rather than fixed. The weight of this self-loop is gated, and the accumulated time scale can also be changed by the input sequence. In this case, even for LSTMs with fixed parameters, the accumulated time scale can be changed by the input sequence because the time constant is the output of the model itself. LSTM has achieved significant success in many areas, such as unconstrained handwriting recognition, speech recognition, handwriting generation, machine translation, header generation and parsing for images.

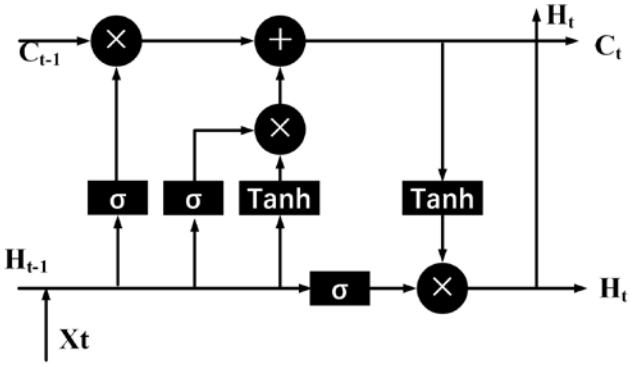

Fig.2 Neural Network LSTM Structure Diagram

3. Dataset Processing

This test uses the Kdd99 dataset. The Kdd99 dataset provides a training set and a test set of 10% training samples and corrected test samples in the KDD99 dataset. This training model uses this training set. The test set is used for the accuracy test, and then used as a reference standard for the evaluation of the effect of the study.

3.1 KDD99 Dataset

In 1998, the US Department of Defense's Advanced Planning Agency (DARPA) conducted an intrusion detection assessment project at the MIT Lincoln Laboratory. Lincoln Labs built a network environment that simulates the US Air Force LAN, collecting nine weeks of TCP dump network connectivity and system audit data, simulating various user types, various network traffic and attack methods, making it Like a real network environment. The raw data collected by these TCP dumps is divided into two parts: 7 weeks of training data contains more than 5,000,000 network connection records, and the remaining 2 weeks of test data contains approximately 2,000,000 network connection records.

A network connection is defined as a sequence of TCP packets from start to finish at a certain time, and during this time, the data is transferred from the source IP address to the destination IP address under a predefined protocol (TCP, UDP). Each network connection is marked as normal or attack. The exception type is subdivided into 39 types of attack types in 4 categories, 22 types of attacks appear in the training set, and 17 unknown attack types appear. In the test set. The four types of exceptions are:

- DOS, denial-of-service. Denial of service attacks, such as ping-of-death, syn flood, smurf, etc.;
- R2L, unauthorized access from a remote machine to a local machine. Unauthorized access from a remote host, such as guessing password;
- U2R, unauthorized access to local superuser privileges by a local unpivileged user. Unauthorized local superuser privileged access, such as buffer overflow attacks;
- PROBING, surveillance and probing, port monitoring or scanning, such as port-scan, ping-sweep, etc.

Professor Sal Stolfo from Columbia University and Professor Wenke Lee from North Carolina State University used data mining techniques to perform feature analysis and data preprocessing on the above data sets to form a new data set. This data set was used in the KDD CUP competition held in 1999 to become the famous KDD99 data set. Although it is a long time ago, the KDD99 dataset is still the fact of the network intrusion detection field Benckmark, laying the foundation for the research of network intrusion detection based on computational intelligence.

The Kdd99 dataset provides a training set and a test set of 10% training samples and corrected test samples in the KDD99 dataset. This training model uses this training set, and uses the test set for accuracy testing, and then A reference standard for evaluating the effectiveness of learning.

3.2 Data Preprocessing

The Kdd99 data set has a total of 41 features, of which three features are character type, and the character data needs to be converted into a numerical type to enable the model to learn. The conversion of the three features is as follows:

- Protocol type

This protocol type is discrete data. There are three types of values: TCP, UDP, and ICMP. The data types are converted to data types corresponding to the value of float type 1.0, 2.0, and 3.0.

- Service. The network service type of the target host

This feature is discrete data. There are 70 values in the Kdd99 dataset. There are three character features, namely 'aol', 'auth', 'bgp', 'courier', 'csnet_ns', 'ctf', 'daytime', 'discard', 'domain', 'domain_u', 'echo', 'eco_i', 'ecr_i', 'efs', 'exec', 'finger', 'ftp', 'ftp_data', 'gopher ', 'harvest', 'hostnames', 'http', 'http_2784', 'http_443', 'http_8001', 'imap4', 'IRC', 'iso_tsap', 'klogin', 'kshell', 'ldap', 'link', 'login', 'mtp', 'name', 'netbios_dgm', 'netbios_ns', 'netbios_ssn', 'netstat', 'nnsp', 'nntp', 'ntp_u', 'other', 'pm_dump ', 'pop_2', 'pop_3', 'printer', 'private', 'red_i', 'remote_job', 'rje', 'shell', 'smtp', 'sql_net', 'ssh', 'sunrpc', 'supdup', 'systat', 'telnet', 'tftp_u', 'tim_i', 'time', 'urh_i', 'urp_i', 'uucp , 'Uucp_path', 'vmnet', 'whois', 'X11', 'Z39_50'. Converted to a numeric type of float type data corresponding to 1.0 to 70.0

- Flag. Connect normal or wrong status

This feature is discrete data. There are 11 values for 'OTH', 'REJ', 'RSTO', 'RSTOS0', 'RSTR', 'S0', 'S1', 'S2', 'S3', 'SF',

'SH'. It indicates whether the connection is started or completed as required by the agreement. For example, SF indicates that the connection is normally established and terminated; S0 indicates that only the SYN request packet is received, and there is no subsequent SYN/ACK. Where SF is normal and the other 10 are error. Converted to a numeric type of float type data 1.0 to 11.0.

- The label

The KDD99 data set mentioned above was obtained by data mining and preprocessing of the DARPA98 data set. However, KDD99 and DARPA98 are not one-to-one correspondence. When Wende Lee and others process the original connection data, some duplicate data is removed.

For example, when a DoS attack is generated, a large number of identical connection records are generated, and only the connection within 5 minutes during the attack process is taken. Record the data set as the type of attack. At the same time, the normal data connection is randomly extracted as a normal data set.

The KDD99 dataset consists of a total of 5 million records, which also provides a 10% training subset and test subset. There are 39 kinds of network attacks in the Kdd99 dataset. In this experiment, we have achieved the purpose of identifying DOS network attacks through LSTM neural network, so we have 10 kinds of apache2, back, land mailbomb, neptune, pod, processtable, smurf, teardrop, udpstorm. The DOS network attack is identified as a value of 1.0. The other twenty-nine network attacks are not in the form of DOS attacks, so they are identified as 0.0. This completes the conversion of the data tag.

3.3 Normalization

Data standardization (normalization) processing is a basic work of data mining. Different evaluation indicators often have different dimensions and dimension units. Such situations will affect the results of data analysis, in order to eliminate the dimension between indicators. Impact, data standardization needs to be done to resolve the comparability of data metrics. After the original data is processed by data standardization, each index is in the same order of magnitude, which is suitable for comprehensive comparative evaluation.

Min-Max Normalization:

Also known as dispersion normalization, it is a linear transformation of the original data, mapping the resulting values between [0 – 1]. The conversion function is as follows:

$$X=(x-\min)/(\max-\min)$$

Where max is the maximum value of the sample data and min is the minimum value of the sample data. One drawback of this approach is that when new data is added, it can cause changes in max and min, which need to be redefined.

4. Neural Network Construction

In this experiment, we used the LSTM neural network and selected three layers of structures, namely the input layer, the hidden layer, and the output layer. Since there are 41 kinds of data features in this experiment, there are 41 neurons in the input layer. The purpose of this experiment is to detect DOS attacks. In fact, it is a two-class problem, so the number of neurons in the output layer is 2, hidden. The number of neurons in the layer is 128. The network structure is shown below

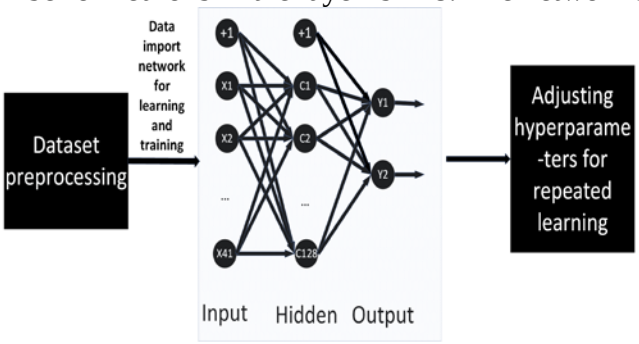

Fig.3 Training Network Data Flow Diagram

5. Hyperparameter Accuracy Comparison and Results Analysis

In this test, it is necessary to adjust the learning rate, batch size, training times, updater and other hyperparameters, and test the accuracy of different hyperparameters to test the hyperparameters. The transfer function of this test uses the softsign function, and the optimization function uses RMSProp, AdaGrad, and momentum to update the data.

First, compare the batch size and the learning rate. The training frequency is set to 64. The optimization function is set to AdaGrad. Select some data to display the list. The detection results are as follows:

TABLE I. Accuracy for batch and learning rate

lr / **batch**	0.001	0.002	0.003	0.004	0.005
30	88.4	88.3	87.6	87.6	86.5
35	89.3	89.1	88.9	87.5	87.1
40	91.2	92.0	91.5	90.2	89.7

It can be concluded from the above table that in the course of multiple engineering learning, when the batch is 40 times and the learning rate is 0.002, the accuracy reaches the maximum value of 92.0. On this basis, the training number and the optimization function are tested and analyzed. The partial results containing the optimal values are displayed. The test results are as follows:

TABLE II. Accuracy for optimizer and epoch

Epoch / **Optimizer**	32	64	96	128	160
RMSProp	85.4	91.7	91.6	91.9	91.8
AdaGrad	87.2	92.0	91.9	91.8	92.0
momentum	86.5	91.2	91.3	91.1	91.2

It can be concluded from the data in the table that when the number of training times is greater than 64 times, the correct rate has converged, and increasing the number of trainings in time cannot

improve the accuracy. In order to improve the training efficiency, this experiment considers that the number of trainings is 64 times. The value has been born.

It can be seen from the above data analysis that the learning rate is 0.002, the training frequency is 64, the optimizer is AdaGrad, and the batch size is 40, the accuracy rate is the highest. This is the optimal solution value of this experiment. This test is a two-category problem. It can be seen from the results that the accuracy is not very high. This is due to the complexity of the network attack itself and the practical application of the neural network in this respect.

References

[1] Zhu Y, Wang X, Zhong E, et al. Discovering Spammers in Social Networks[C]// Aaai Conference on Artificial Intelligence. 2012.

[2] Kale M, Choudhari D M. DDOS attack detection based on an ensemble of neural classifier [J]. IJC- SNS, 2014, 14(7): 122-128.

[3] Saied A, Overill R E, Radzik T. Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept[C]// International Conference on Practical Applications of Agents & Multi-agent Systems. Springer, Cham, 2014.

[4] Gupta B B , Joshi R C , Misra M , et al. Predicting Number of Zombies in a DDoS Attack Using ANN Based Scheme[M]// Information Technology and Mobile Communication. Springer Berlin Heidelberg, 2011.

[5] Karimazad R, Faraahi A. An anomaly-Based meth— od for DDoS attacks detection using RBF neural networks[C]//Proceedings of 2011 1st International Conference on Network and Electronics Engineering. Singapore: IACSIT, 2012.

[6] Oke G , Loukas G , Gelenbe E . Detecting denial of service attacks with Bayesian classifiers and the random neural network [J]. 2007.

[7] Gupta B, Badve O P. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment [J]. Neural Computing & Applications, 2017, 28(12):3655-3682.

[8] Akoglu L, Tong H, Koutra D. Graph-based Anomaly Detection and Description: A Survey [J]. Data Mining & Knowledge Discovery, 2015, 29(3):626-688.

[9] Ferrara E. Measurement and Analysis of Online Social Networks Systems [M]. Springer New York, 2014.