International Journal of LNCT
Volume-6 Issue-28 February -2022
ISSN: (Online):2456-9895

Design a novel algorithm for Intrusion Detection Model Using Recurrent Neural Networks

Avani Bhoyar[1] , Mr. Vinod Patel[2]
[1]*Computer science department, Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh, India (affiliated by AICTE,RGPV)*
E-Mail: bhoyaravani1503@gmail.com
[2]*Computer science department, Lakshmi Narain College of Technology, Bhopal, Madhya Pradesh, India (affiliated by AICTE,RGPV)*
E-Mail : vinodp@lnct.ac.in

Abstract
The malicious activity and policy violations on network of systems is continuously monitored by device or software application called IDS passively monitor the data and uncover any potentially disastrous connection. Technically IDS are aimed at serving three important security functions i.e., monitoring the data, unearthingany potentially harmful transactions and finally responding to unauthorized activity. With the gigantic structure of the Internet, its distributed nature and lack of central security mechanism, the prevention of attacks is not possible and therefore detection and recovery from attacks become indispensable. The IDS does exactly as the name suggests, it detects the possible intrusion. To study the impacts of application of the wavelets on the detection coverage of Recurrent Neural Networks classification model for network Intrusion Detection.

Keywords:
Intrusion Detection, Recurrent Neural Networks.

1. INTRODUCTION

Intrusion is defined as the set of activities aimed at bypassing the security mechanism of the computer networks and systems. Detecting intrusions is an inescapable step in taking the corrective actions. The process of monitoring the network connection to uncover the possible intrusions is called the Intrusion Detection and the system with which the responsibility of detecting intrusions from the network traffic lies is called IDS. Intrusions are aimed at compromising one or more of the three basic security goals of the network system: confidentiality, availability and integrity[1]. The user from the outer world Internet to gain access to the system, or the legitimate and authorized user with the intention of gaining additional privileges, and the authorized users misusing the privileges given to them can initiate intrusions. classify attacks into seven broad groups as given below:

• Infection: This attack is aimed at installing the harmful files or tampering the valid files thereby infecting the files. These attacks can be further sub-categorized as viruses, worms, and trojans etc.

• Exploding: This attack is aimed at overflowing the victim with bugs, the prominent attack of this type is buffer-overflow[2].

• Probe: This attack is aimed at collecting vital information about the network so as to identify the potential entry points that can be compromised. Some information of interest for an attacker can be to check which services are running, what Internet Protocols (IP) addresses are working currently. Some attacks falling in this class are Port Scan, IP scan and Nmap.

• Cheat: These attacks are aimed at gaining access to the network by impersonation i.e., by providing a fake identity to access secured files of the system. Some of the attacks falling in this class are IP Spoofing, Session Hijacking etc.

• Traverse: The attacks of this type attempt to break into the system by performing a password matching against all the possible passwords. Dictionary attacks and brute force attacks are a few examples of this type.

• Concurrency: Attacks of this type capitalize on one or more weaknesses of the system to carry out some disastrous actions. A prominent attack of this system is DDoS wherein system resources are exhausted, so as to deny it serving the legitimate users.

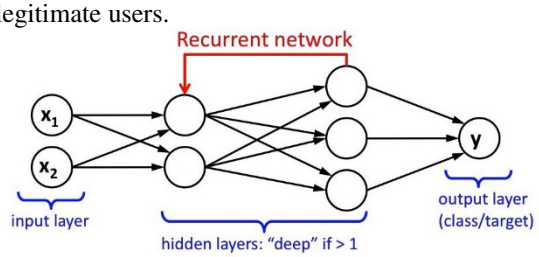

Figure 1: Recurrent neural network

various categories based on their carrier, and the most popular carrier of the attacks has been malware A typical network configuration is depicted. In this network layout, a network is connected to an external network, there is a firewall to filter the disastrous connection originating from the outer world directed towards the network. The firewall is the first line of defense to block any harmful connections. As can be seen from the figure, gateways are positioned at the entry of the network, so technically they are able to filter out

the connections that originate from / directed to a host in the outside world. IDS's are positioned inside the network, rather than blocking[3] the network connections. It is aimed at analyzing the network connections for the possible harmful connections. IDS is aimed at unearthing potentially harmful connections that have somehow sneaked through the firewall. An IDS checks[4] for the possible network attacks and initiates the corrective approach by alerting the system admin.

2. RELATED WORK

- Anomaly Detection for IDS

Anomaly-based detection methods are based on the analysis of the profiles that represent the normal traffic behavior. These methods were pushed in with the aim of detecting the zero-day attacks without human intervention. These models commence by monitoring network traffic over a span of time and thereafter creating a baseline profile for the legitimate traffic. Subsequently, any new activity that deviates from the normal profile is considered to be anomalous. The potential problem with this system is too many false alarms, for they are incapable of handling the concept drift. Even a slight variation from the normal profile will be reported as an anomaly. A varied set of techniques has been applied to develop the anomaly-based systems, among the most popular techniques, in this review, we document only the models based on statistical and Machine Learning methods.

2.1 STATISTICAL METHODS

The statistical models are based on the idea of maintaining two system profiles during the course of anomaly detection. The two statistical profiles consist of the currently observed and previously stored statistical profile based on certain variables of the system over time.

Statistical models build a profile for the normal traffic activity and compare the observed behavior of the network to the recent behavior, and if there is a significant deviation of the current behavior from the recent behavior, it is treated as anomalous otherwise the behavior is considered to be normal.
The methodology behind statistical method is that it fits in a statistical model for the training data and run over a statistical deduction test for each of the unseen data to predict the class of the unseen data [5] The instances which score very low probability in the deduction test by the learned model are declared as anomalies. Statistical model includes parametric and non-parametric techniques to build the learning model. Parametric techniques try to learn things by analyzing the distribution of the input data whereas the non-parametric techniques don't presume the knowledge from the distribution of the data [6].
[7] designed a learning model using three expectation-maximization algorithms that utilized statistical anomaly detection method, accounting on the difference between the attributes. They partitioned data attributes into indicator attributes and environmental attributes established over the certainty of the user deciding which attributes represent an anomaly. The indicator attribute was designed to learn the environment and read the subsequent data instances, and classify accordingly, whether it is an anomaly or not. The indicator attributes were ignored if they weren't conditioned over the environmental attributes in statistical approach. The model had high precision and recall value but still subject-able to learn environment in all the circumstances.
[8] functioned an unconditional α-stable first order model and statistical hypothesis testing to filter out the anomalies in the network traffic. The marginal distribution of the original traffic was modeled and functioned by the α-stable function and classified by Generalized Likelihood ratio test. The proposed work identified anomaly such as flash-crowds and floods. As extension of this work[9] used in addition a non-parametric adaptive cumulative sum method for the statistical calculation and detection of anomalies in the network traffic.
A flow-based statistical IDS called Flow-based Statistical Aggregation Scheme (FSAS) was built by encompassing two parts, namely, feature generator and flow-based detector. The feature generator was modeled to collect the network traffic

and reports were generated by event handlers and provided to the flow management module, which decided whether the packet is part of the flow or it needs to be generated as new flow key [10]. The flow keys were inspected and were accumulated together and dynamic updating was done as per flow keys. The event time module converted the flows into the format acceptable to the statistical model. The score vectors were based on the maliciousness of data, and were rated by neural network classifier, such that, if the flow had higher malicious data, then it was rated with higher probability of being an attack.

3. PROPOSED METHODOLGY

The RNN architecture[9] is the addition of sequential information to the feedforward neural network. The RNN performs the same task for each part. This is why it is called a recurrent network; the output is dependent upon the previous computation. The hidden computation of RNN[11][12] is computed as given below: where denotes the hidden state vector at time t; σ is the activation function, also known as the nonlinearity function[13]; is the hidden weight matrix[14][15]; is the hidden to hidden weight matrix; is the input vector at time t; and is the bias term.

$$H_t = \sigma\left(Wx_t + VH_{t-1} + b_H\right),\ t = T, \ldots, 1,$$

Working of proposed approach[16] Let us assume that there is a random variable X taking on N different values. Let us assume that out of the N values there are in total n unique values[16] a feature X can take. One of the working hypothesis for this work is that if,

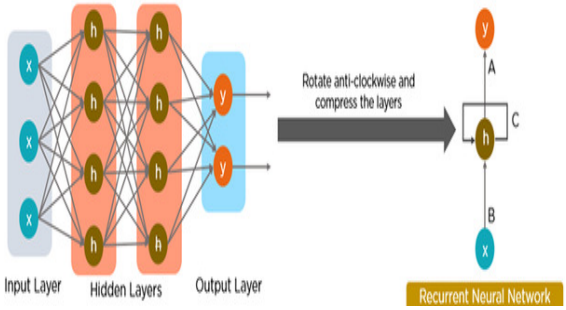

Figure 2: Working of RNN algorithm

- n tends towards infinity if the feature[17][18] is quantitative.
- n tends to a finite constant (the number of modalities) if the feature is qualitative.In practice, at all the times we have the cases where N ≥ n. **Constraints on** N
- N cannot be infinite as there is always a limit on N[19].

- In an effort to differentiate between the two types of variables, N must not be too small because for the small values of N, the two types of variables will have the same behavior[20].
- N cannot be too large: If N ≤ Measurement limit or if N ≤ Media limit, the increasing behavior of n = f(N).

3.1 RESULTS

After reducing the data-set the next step is to check out how good or bad the RNN[21] has reduced the data-set. As the purpose of this research work is to enhance the detection rate for RNN[22] model by applying RNN[23]. It is already well established that the main aimof the work is not actually to reduce the dimension but to enhance the detection rate. DR is simply used as a tool[24] to enhance the detection rate. The next logical step is to test the classifier model for IDS. In this work RNN[25] with non-linear kernel, i.e., Radial Basis[26] function is used to develop the model. The reason for choosing RNN is that it has a rich set of kernel functions that can be used effectively with the different data. The RNN model[27] is trained with a series of gamma bandwidths and the best result of the bestone is retained[28]. For testing the model, a 10-fold cross-validation is applied. The results of the model are evaluated in terms of Precision, Recall, ROC[28] etc. Moreover, Johns Quality[29] Assignment Curve[30] is used to check the effectiveness of the proposed model.

3.2 CONDITIONS OF CONFUSION MATRIX

Confusion matrix is a simple 2 × 2 matrix producing four outcomes which is used commonly in almost all machine learning evaluation. The outcome of the confusion matrix indicates the True Positive, True Negative, False Positive and False Negative measures (Hay, 1988). The Figure 4.2 represents the confusion matrix for IDS, where

True Positive ($AT \rightarrow AT$): Cases where the Attack (AT) instance is correctly classified as an Attack (AT) instance.

- True Negative ($NR \rightarrow NR$): Cases where the Normal (NR) instance is correctly classified as Normal (NR) instance.

- False Positive ($NR \rightarrow AT$): Cases where the Normal (NR) instance is incorrectly classified as an Attack (AT) instance.

- False Negative ($AT \rightarrow NR$): Cases where the Attack (AT) instance is incorrectly classified as Normal (NR) instance.

Assigned clusters in 0.312 seconds

Accuracy 91.719 % Confusion Matrix:

[[225790 24646]
[1110 59483]]

Classification Scores:

	precision	recall	f1-score	support
anomaly	1.00	0.90	0.95	250436
normal.	0.71	0.98	0.82	60593
avg / total	1.71	1.88	1.77	311029

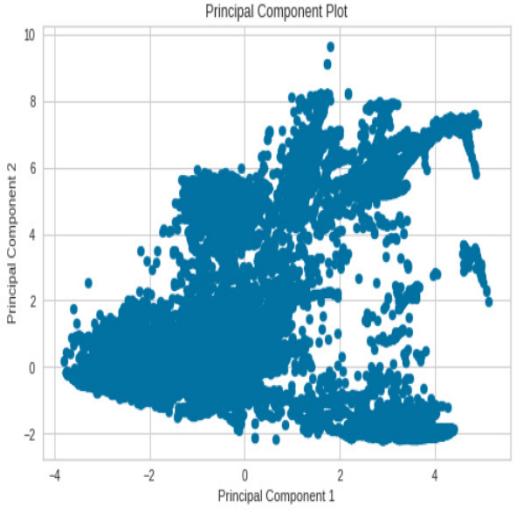

Figure 3: RNN with principle component plot

4. CONCLUSION

Once the traffic has been captured and pre-processed by the capturing unit, the next step in the process is attack detection. At the heart of an IDS is a detection methodology which can be based on anomaly detection or misuse detection, hence at this point a proposed can have a signature matching technique or anomaly detection. If its going to be the signature matching techniques, the signature database should be available, and if its going to be anomaly detection, the model for normal data has to be in place. For each connection, detection module classifies it as either an attack or a valid network connection.

REFERENCES

[1]. V. K. Kukkala, S. V. Thiruloga and S. Pasricha, "INDRA: Intrusion Detection Using Recurrent Autoencoders in Automotive Embedded Systems," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3698-3710, Nov. 2020, doi: 10.1109/TCAD.2020.3012749.

[2]. N. Mboula and E. Nogues, "IDrISS: Intrusion Detection for IT Systems Security : Toward a semantic modelling of side-channel signals," 2020 28th European Signal Processing Conference (EUSIPCO), 2021, pp. 735-739, doi: 10.23919/Eusipco47968.2020.9287662.

[3]. A. Prabhu, H. N. Champa and D. Kalasapura, "Network Intrusion Detection Using Sequence Models," 2019 Grace Hopper Celebration India (GHCI), 2019, pp. 1-5, doi: 10.1109/GHCI47972.2019.9071806.

[4]. R. Vinayakumar, K. P. Soman and P. Poornachandran, "Applying convolutional neural network for network intrusion detection," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1222-1228, doi: 10.1109/ICACCI.2017.8126009.

[5]. S. Althubiti, W. Nick, J. Mason, X. Yuan and A. Esterline, "Applying Long Short-Term Memory Recurrent Neural Network for Intrusion Detection," Southeast on 2018, 2018, pp. 1-5, doi: 10.1109/SECON.2018.8478898.

[6]. P. Singh, J. J. P, A. Pankaj and R. Mitra, "Edge-Detect: Edge-Centric Network Intrusion Detection using Deep Neural Network," 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), 2021, pp. 1-6, doi: 10.1109/CCNC49032.2021.9369469.

[7]. S. Nayyar, S. Arora and M. Singh, "Recurrent Neural Network Based Intrusion Detection System," 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 0136-0140, doi: 10.1109/ICCSP48568.2020.9182099.

[8]. A. Kotian, S. Patil, N. Prajapati and Y. Mane, "Realtime Detection Of Network Anomalies Using Neural Network," 2020 International Conference on Smart Technologies in Computing, Electrical and Electronics (ICSTCEE), 2020, pp. 240-245, doi: 10.1109/ICSTCEE49637.2020.9276931.

[9]. Marwan Ali Albahar, "Recurrent Neural Network Model Based on a New

Regularization Technique for Real-Time Intrusion Detection in SDN Environments", Security and Communication Networks, vol. 2019, Article ID 8939041, 9 pages, 2019. https://doi.org/10.1155/2019/8939041

[10]. M. Tan, A. Iacovazzi, N. M. Cheung and Y. Elovici, "A Neural Attention Model for Real-Time Network Intrusion Detection," 2019 IEEE 44th Conference on Local Computer Networks (LCN), 2019, pp. 291-299, doi: 10.1109/LCN44214.2019.8990890.

[11]. S. K. Alabugin and A. N. Sokolov, "Applying of Recurrent Neural Networks for Industrial Processes Anomaly Detection," 2021 Ural Symposium on Biomedical Engineering, Radio electronics and Information Technology (USBEREIT), 2021, pp. 0467-0470, doi: 10.1109/USBEREIT51232.2021.9455060.

[12]. A. N. Sokolov, S. K. Alabugin and I. A. Pyatnitsky, "Traffic Modeling by Recurrent Neural Networks for Intrusion Detection in Industrial Control Systems," 2019 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM), 2019, pp. 1-5, doi: 10.1109/ICIEAM.2019.8742961.

[13]. B. Roy and H. Cheung, "A Deep Learning Approach for Intrusion Detection in Internet of Things using Bi-Directional Long Short-Term Memory Recurrent Neural Network," 2018 28th International Telecommunication Networks and Applications Conference (ITNAC), 2018, pp. 1-6, doi: 10.1109/ATNAC.2018.8615294.

[14]. T. Ishitaki, R. Obukata, T. Oda and L. Barolli, "Application of Deep Recurrent Neural Networks for Prediction of User Behavior in Tor Networks," 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), 2017, pp. 238-243, doi: 10.1109/WAINA.2017.63.

[15]. S. Naseer et al., "Enhanced Network Anomaly Detection Based on Deep Neural Networks," in IEEE Access, vol. 6, pp. 48231-48246, 2018, doi: 10.1109/ACCESS.2018.2863036.

[16]. Rajawat A.S., Rawat R., Barhanpurkar K., Shaw R.N., Ghosh A. (2021) Vulnerability Analysis at Industrial Internet of Things Platform on Dark Web Network Using Computational Intelligence. In: Bansal J.C., Paprzycki M., Bianchini M., Das S. (eds) Computationally Intelligent Systems and their Applications. Studies in Computational Intelligence, vol 950. Springer, Singapore. https://doi.org/10.1007/978-981-16-0407-2_4

[17]. V. K. Kukkala, S. V. Thiruloga and S. Pasricha, "INDRA: Intrusion Detection Using Recurrent Autoencoders in Automotive Embedded Systems," in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, no. 11, pp. 3698-3710, Nov. 2020, doi: 10.1109/TCAD.2020.3012749.

[18]. S. H. Park, H. J. Park and Y. Choi, "RNN-based Prediction for Network Intrusion Detection," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2020, pp. 572-574, doi: 10.1109/ICAIIC48513.2020.9065249.

[19]. S. N. Pakanzad and H. Monkaresi, "Providing a Hybrid Approach for Detecting Malicious Traffic on the Computer Networks Using Convolutional Neural Networks," 2020 28th Iranian Conference on Electrical Engineering (ICEE), 2020, pp. 1-6, doi: 10.1109/ICEE50131.2020.9260686.

[20]. A. A. Abdul Lateef, S. T. Faraj Al-Janabi and B. Al-Khateeb, "Hybrid Intrusion Detection System Based on Deep Learning," 2020 International Conference on Data Analytics for Business and Industry: Way Towards a Sustainable Economy (ICDABI), 2020, pp. 1-5, doi: 10.1109/ICDABI51230.2020.9325669.

[21]. A. Singh Rajawat and S. Jain, "Fusion Deep Learning Based on Back Propagation Neural Network for Personalization," 2nd International Conference on Data, Engineering and Applications (IDEA), 2020, pp. 1-7, doi: 10.1109/IDEA49133.2020.9170693.

[22]. Kaur, S., Singh, M. Hybrid intrusion detection and signature generation using Deep Recurrent Neural Networks. *Neural Computer & Applica* **32,** 7859–7877 (2020). https://doi.org/10.1007/s00521-019-04187-9

[23]. Atefinia, R., Ahmadi, M.

Network intrusion detection using multi-architectural modular deep neural network. J Supercomput 77, 3571–3593 (2021). https://doi.org/10.1007/s11227-020-03410-y

[24]. Rajawat A.S., Rawat R., Barhanpurkar K., Shaw R.N., Ghosh A. (2021) Blockchain-Based Model for Expanding IoT Device Data Security. In: Bansal J.C., Fung L.C.C., Simic M., Ghosh A. (eds) Advances in Applications of Data-Driven Computing. Advances in Intelligent Systems and Computing, vol 1319. Springer, Singapore. https://doi.org/10.1007/978-981-33-6919-1_5

[25]. Drewek-Ossowicka, A., Pietrołaj, M. & Rumiński, J. A survey of neural networks usage for intrusion detection systems. J Ambient Intel Human Computer 12, 497–514 (2021). https://doi.org/10.1007/s12652-020-02014-x

[26]. Shokoohsaljooghi, A., Mirvaziri, H. Performance improvement of intrusion detection system using neural networks and particle swarm optimization algorithms. Int. j. inf. techno. 12, 849–860 (2020). https://doi.org/10.1007/s41870-019-00315-9

[27]. Thakkar, A., Lohiya, R. A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions. Artif Intel Rev (2021). https://doi.org/10.1007/s10462-021-10037-9

[28]. Rajkumar N., D'Souza A., Alex S., Kathrine G.J.W. (2019) Long Short-Term Memory-Based Recurrent Neural Network Approach for Intrusion Detection. In: Pandian D., Fernando X., Baig Z., Shi F. (eds) Proceedings of the International Conference on ISMAC in Computational Vision and Bio-Engineering 2018 (ISMAC-CVB). ISMAC 2018. Lecture Notes in Computational Vision and Biomechanics, vol 30. Springer, Cham. https://doi.org/10.1007/978-3-030-00665-5_81

[29]. Rajawat A.S., Barhanpurkar K., Shaw R.N., Ghosh A. (2021) Risk Detection in Wireless Body Sensor Networks for Health Monitoring Using Hybrid Deep Learning. In: Mekhilef S., Favorskaya M., Pandey R.K., Shaw R.N. (eds) Innovations in Electrical and Electronic Engineering. Lecture Notes in Electrical Engineering, vol 756. Springer, Singapore. https://doi.org/10.1007/978-981-16-0749-3_54

[30]. Hsu CM., Hsieh HY., Prakosa S.W., Azhari M.Z., Leu JS. (2019) Using Long-Short-Term Memory Based Convolutional Neural Networks for Network Intrusion Detection. In: Chen JL., Pang AC., Deng DJ., Lin CC. (eds) Wireless Internet. WICON 2018. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 264. Springer, Cham. https://doi.org/10.1007/978-3-030-06158-6_9

[31]. Maseleno A., Abdullah D., Satria E., Souisa F.N.J., Rahim R. (2021) An Intelligent Intrusion Detection for Smart Cities Application Based on Random Optimization with Recurrent Network. In: Elhoseny M., Shankar K., Abdel-Basset M. (eds) Artificial Intelligence Applications for Smart Societies. Studies in Distributed Intelligence. Springer, Cham. https://doi.org/10.1007/978-3-030-63068-3_8