Turkish Journal of Computer and Mathematics Education *Vol.12 No.3(2021), 3945-3949*

Research Article

CNN Intrusion Detection for Threat Analysis of a Network

Tressa Michael[a]

[a]Assistant Professor, Department of Electronics and Communication Engineering, Rajagiri School of Engineering and Technology, Kakkanad, Kerala, India.

Article History: Received: 10 November 2020; Revised 12 January 2021 Accepted: 27 January 2021; Published online: 5 April 2021

Abstract: The technological advancement realized in the discovery and embrace of both IoT and IIoT is totally indispensable. Many systems and subsystems both robust and miniaturized have made their existence into the technical arena due to IoT. It goes without saying that IoT has brought into light very diverse benefits that cut across universal applications.However, the pre-requisite of a network channel existence for an IoT operation to be successful is the only pitfall that this essentially unique system possesses. There is a significant amount of danger associated with transmission networks. They have very substantial susceptibility to both online and offline threats by malicious cyber intentions.This paper focuses on the analyses of the threats posed to these IoT networks through Artificial Neural Networks. Specifically, a model is trained through recurrent and convolutional neural network to do intensive analysis on the threat intensity, type and threat source for data logging purposes. The Intruder detection system (IDS) explored in this paper registers a success rate of 99% based on the empirical data posed to the model.

Keywords: Threat analysis, Intruder detection system, CNN, KDD dataset.

1. Introduction

The rise in the potential threats of network-imposed activities such as IOT and IIOT has prompted several studies in the field of IDS (Intruder detection systems) (Ahsan, M., 2020). This has specifically and extensively taken effect in the subdiscipline of Artificial Intelligence and Artificial Neural Networks (Estaran, J., 2016). Models have been trained to analyses empirical data used in the study of IDS (Ivanov, A., 2017). The intelligent system developed has relational convolution with existing models and the data commonly used is KDD dataset which was developed in 1998 for study of threat analysis. This era has seen various trained models producing very substantial output in network protection from intrusion.

However, there are still cases of network intrusion. This is despite the various artificial intelligence techniques that have developed over the years to curb such occurrences. Day in day out various advancements and adjustments occur in the network configuration protocols in the effort to enhance it but in the real sense there is a disadvantage of weakening the protocols with or without knowledge.

Intrusions such as malware commonly take advantage of very tiny changes made to the original bedrock development codes that have been built as the basis of running and maintaining the networks. The adjustments are necessary but at a very costly exposure.

It is time to reconsider the threat management procedure. The method proposed in this paper is essentially to analyses the threats and follow up steps can be taken to make the full model responsive to the incoming threats.

2. Threat Analysis

The threat analysis is carried on the basis of the following subdisciplines:

2.1 Type of Threats

The RNN and CNN artificial neural algorithm used in this situation is used to specify the type of the threat that is supposedly imposed on the network. It groups the threats as follows.

(1) Malware-This is an executable file made accessible to the network user by the attacker. This file once loaded into the Operating system of the device it is used by the attacker to gather very sensitive information thus imposing very serious repercussions to the user. Details such as financial and social are at risk of being in the wrong hands once this kind of threat is obtained in the network. It also generally disrupts the smooth operation of the system, delaying signals, or even initiates much unsupervised instructions for devices.

(2) Data Loopholes-These are the breaches that are available in the network especially in offline communication networks like Bluetooth and networks. The packets of communication are invaded and very sensitive information is retrieved posing very great danger to the user.

Feeble IOT network outlines-Lack of network pervasiveness which is a common design procedure for IOT networks has endangered them to malicious attack.

(4) Denial of Service-This is a situation where there is requested persisted entry even though there is denial by the network server. There are various attempts to make entry into the network. This can be fathomed numerically by the continuous input of wrong passwords for a continuous period.

2.2 Intruder Type

The type of intruder trying to intoxicate the network can be identified and grouped as follows:

(1) External intruder-This is an intruder who is from an outside network which is not the network they are trying to intoxicate. They use other networks but come to the network to distribute various threats to retrieve information and so on.

(2) Internal networks-This is an intruder who is from the network of investigation and is specifically interested to disrupt the smooth-running activities of users in the networks.

2.3.Internet Connectivity

(1) Online Intruder -The threat is classified to be coming from an online source. Normally this is very common since they take advantage of very common IP addresses and they can easily get to steal information from users of the addresses by interfering with the coded background of the networks.

(2) Offline Intruder-This is an intruder who has access to the network without internet connectivity. There's very little technology to handle and counter attack this kind of intrusion threat but this is a very dangerous group of individuals.

2.4 Intensity of Threat

This is a classification basis that gives information on the level of intensity presented by the threat. How dangerous is the threat? This is very necessary information to initiate counter offers that will enable timely curb of the imminent dangers. Colour codes are used to indicate that level of the threat.

COLOUR	INDICATION
RED	Very dangerous threat. Action prompted!!
GREEN	Dangerous threat. Action prompted
YELLOW	Mid range threat. Action prompted.
BROWN	Low threat. Action needed.
MAROON	Very low threat. Action needed.

Fig.1. Intensity of Threat

2.5 Proximity of the Threat

This information is necessary to show how close the user of a network is close to the threat that is described in the analyses. Unfortunately, this process is available for same network users. For the case of the external intrusion, it would be comparatively hard to make this conclusion due to difference in network operation.

3. Related Work

There have been numerous attempts to make a cut into the IDS studies. Traditional learning models of machine learning have been indulged into this extensive arena. The commonest application is the K nearest Neighbour (KNN). They however have not been able to capture the reality in terms of the dynamics involved in the network system. Deep learning algorithms have also been incorporated into this study. The advantage they have over the traditional methods is the capability to intensively study the behavioural dynamics of a network and at the same time do very defined classification. An example is the auto encoder development which was a big step in the IDS studies. Neural networks have made significant subway into the network protection mechanisms. Recurrent Neural Network has been used to be reconstitute a combine method spectral grouping and model training for intrusion detection. A combination of deep autoencoder for extraction of features and network neural feedforward we used inclusively for clustering intrusion detection.

These deep learning developments captured the classification parameters without delving deep into the analysis of the threats imposed and their solutions. The proposed solution in this paper offers a solution for the deep analyses specifically for two methods of ANN that is Recurrent Neural Network and Convolutional Neural Network. All this is aimed at supplementing the work of research predecessors in the Intrusion Detection systems.

4. Algorithms Used

4.1 Methodology

The methodology is summarised in the diagram below.

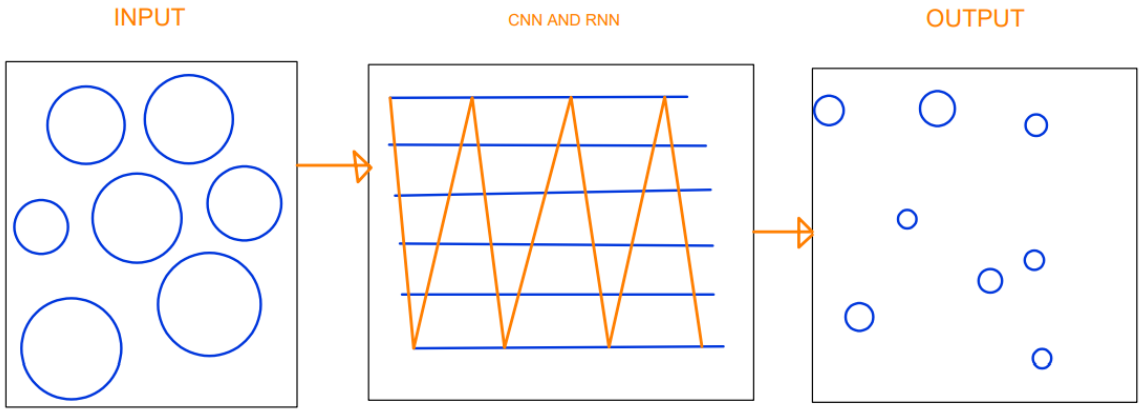


Fig.2. Methodology

The input threat is subjected to the combination architecture of RNN and CNN that chucks that data into bits to carry out the threat analysis. The data has gaussian relation and it is assumed that the resultant output is a gaussian distribution but in very detailed format once the classification and the regrouping has occurred. The algorithms used are:

4.1.1 Levenberg-Marquardt Algorithm

This algorithm has been used for optimisation of the neural network and it is very applicable due to the threat being quantified in the summation basis. The intrusion is expressed as a sum of different mini threats that sums up to exceed a limit where it is numerically considered a threat.

The neural Network has been trained with an input that specifies a certain target since we want a predefined category of different clustering.

4.1.2 BFGS-Algorithm

This optimisation method has lateral dependency on single domain infiltration. The logical flow followed in this network is that the network is a single domain that has been infiltrated by noise which in this case is assigned to the threat in question. The model is trained to carry out an optimisation method for the full analysis.

$$\min_{x\in\mathbb{R}^d} F(x) = \int f(x;z,y)dP(z,y),$$

$$R(x) = \frac{1}{N}\sum_{i=1}^{N} f(x; z^i, y^i) \triangleq \frac{1}{N}\sum_{i=1}^{N} F_i(x),$$

$$x_{k+1} = x_k - \alpha_k H_k g_k^{S_k},$$

$$g_k^{S_k} = \nabla F_{S_k}(x_k) \triangleq \frac{1}{|S_k|}\sum_{i \in S_k} \nabla F_i(x_k),$$

$$\mathbb{E}_k\left[(H_k \nabla F(x_k))^T (H_k g_k^{S_k})\right] = \|H_k \nabla F(x_k)\|^2,$$

$$\mathbb{E}_k\left[\left((H_k \nabla F(x_k))^T (H_k g_k^{S_k}) - \|H_k \nabla F(x_k)\|^2\right)^2\right] \leq \theta^2 \|H_k \nabla F(x_k)\|^4,$$

$$\frac{\mathrm{Var}_{i \in S_k^v}\left((g_k^i)^T H_k^2 g_k^{S_k}\right)}{|S_k|} \leq \theta^2 \left\|H_k g_k^{S_k}\right\|^4,$$

$$\frac{\sum_{i \in S_k^v}\left((g_k^i)^T H_k^2 g_k^{S_k} - \left\|H_k g_k^{S_k}\right\|^2\right)^2}{|S_k^v| - 1}.$$

4.1.3 Feed forward algorithm

Suits the study because the connections used in the nodes do not in any way form a rotational back dependency. It is used to train the model for nonlinear optimisation. Mathematically it is as shown below

$$f(x) = \frac{1}{1 + e^{-x}}$$

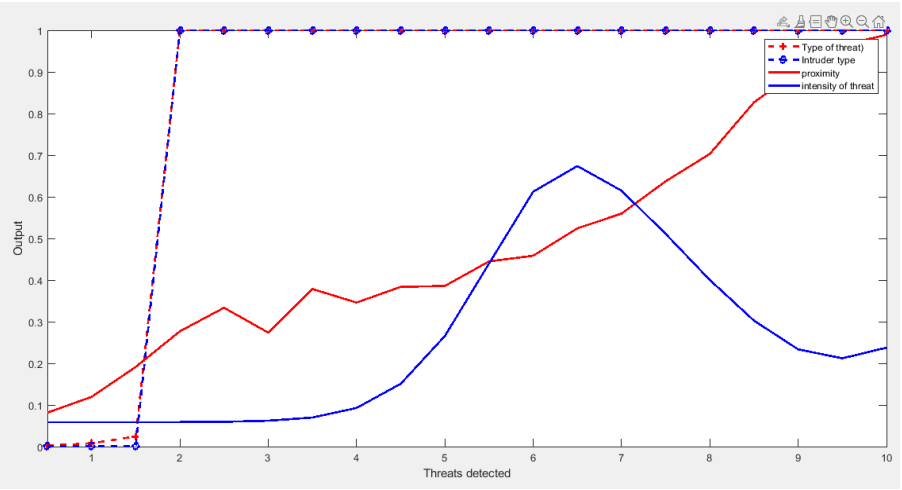
$$f'(x) = f(x)(1 - f(x)).$$

4.1.4 Backward Learning Algorithm

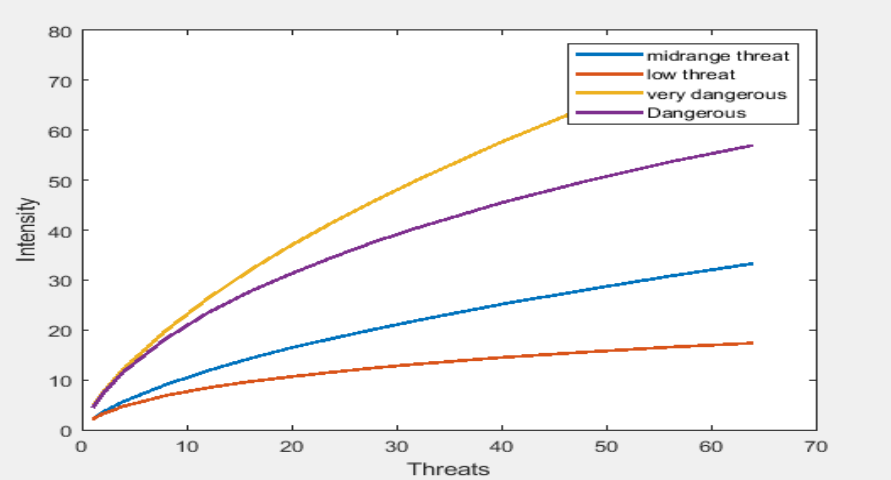
Used to counter the effects of the feed forward algorithm for training the model. The feed forward is mostly based on derivative function hence anticipation. Backward training uses integration techniques of optimisation for the model.

For the jacobian Matrix application it minimises J and hence optimise the cost function.

5. Results and Discussion



(a)



(b)

Fig.3. Comparison of Results

The results indicate the numerical output gotten from running the two neural networks of RNN and CNN.As can be seen the full input is subjected into two robust neural platforms that optimise the model which has been trained using the learning algorithms and the output realised is the classification of the threats and the threats are also assigned subfolders that show their intensity.

6. Conclusion

In this paper a solved outcome was modelled based on RNN and CNN for the IDS system. It has full incorporation of the learning models requested by many network providers. The results, as explained earlier were full focused on numerically analysis the data configuration of the threat registered and then classifying it into readable forms that can then be used by fraternities to take immediate action either in-house or externally.

A future recommendation would be to find a way to analyse threats registered by offline cyber-attacks. Our model restricted the study to only online attacks which would very much be addressed.

References

Ahsan, M. (2020). Convolutional Neural Networks with LSTM for Intrusion Detection. EPIC Series in Computing, 69-79.

Cheng, C. (2017). Maximum Resilience of Artificial Neural Networks. International Symposium on Automated Technology for Verification and Analysis, 251-268.

Estaran, J. (2016). Artificial Neural Networks for Linear and Non-Linear Impairment Mitigation in High-Baudrate IM/DD Systems. ECOC 2016; 42nd European Conference on Optical Communication, 1-25.

Gerven, M. (2017). Editorial: Artificial Neural Networks as Models of Neural Information Processing. Frontiers in Computational Neuroscience, N.P.

Hajian, A. (2018). Application of Soft Computing and Intelligent Methods in Geophysics. Artificial Neural Networks, 3-69.

Hodo, E. (2013). Threat Analysis of IoT Networks using Artificial Neural Network Intrusion Detection System. 232-236.

Ivanov, A. (2017). Evaluation of Signature Verification Reliability based on Artificial Neural Networks, Bayesian Multivariate Functional and Quadratic Forms. Computer Optics, 765-774.

Khoo, Y. (2018). Solving Parametric PDE Problems with Artificial Neural Networks. Mathematics, N.P.

Silva, I. (2016). Artificial Neural Network Architectures and Training Processes. Artificial Neural Networks, 21-28.

Troyer, M. (2017). Solving the Quantum Many-body Problem with Artificial Neural Networks. Science, N.P.

Walczak, S. (2019). Artificial Neural Networks. Florida.

Wanto, A. (2017). Use of Binary Sigmoid Function and Linear Identity in Artificial Neural Networks for Forecasting Population Density. International Journal of Information System & Technology, N.P