A Deep Learning Approach For Anomaly Detection in Data Communication Network

T.Thameera and K.Thabotharan
Department of Computer Science, University of Jaffna
thameera808@gmail.com,thabo@univ.jfn.ac.lk

Introduction

Cyber attack incidents are rapidly increasing with the use of internet. A Network Intrusion Detection System (NIDS) monitors network traffic searching for suspicious activity and known threats, sending up alerts when it finds such items. It can be categorized into anomaly detection and misuse detection.

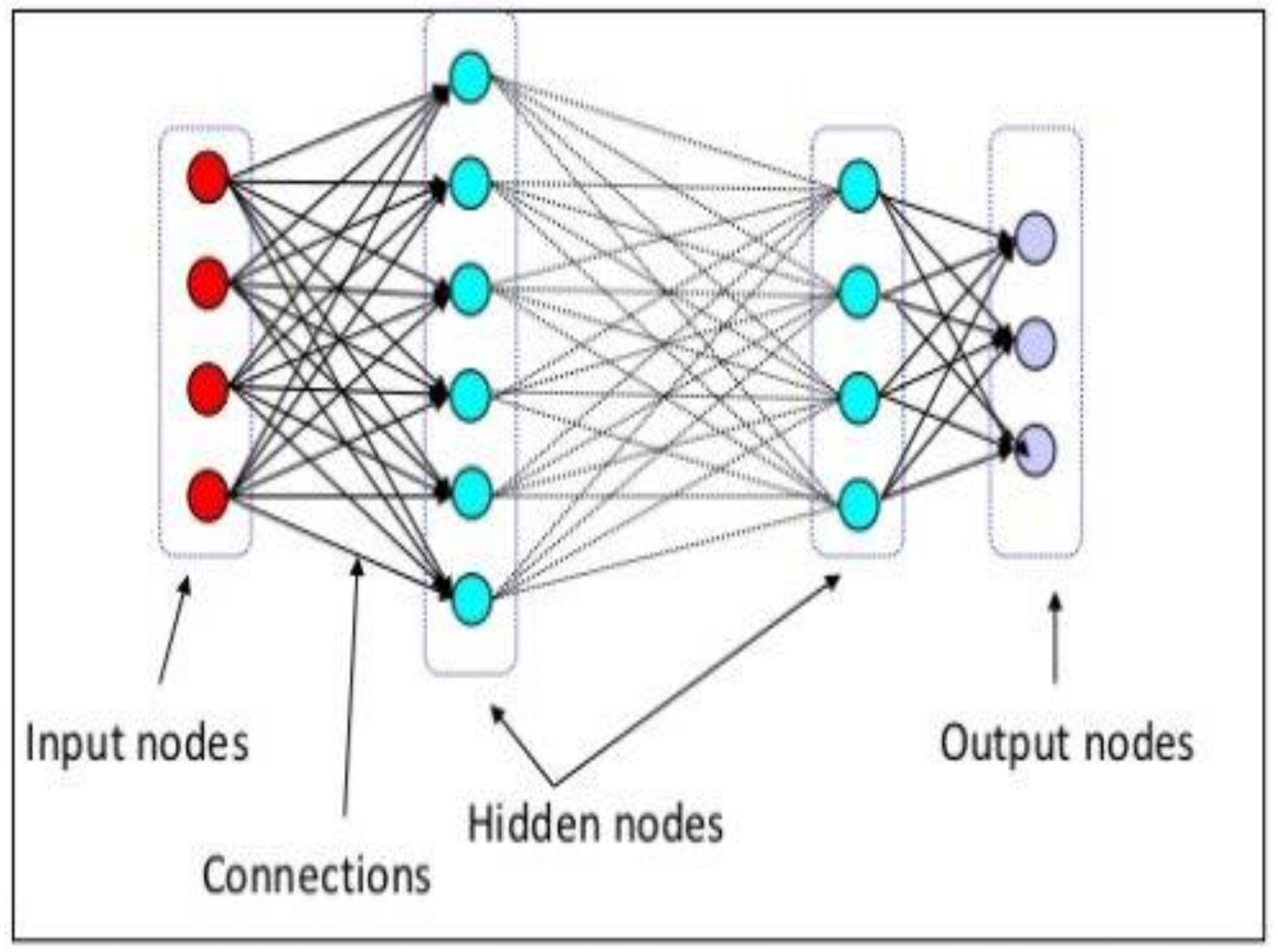
- Misuse detection uses the known attack patterns to identify attacks and shows high accuracy with less false alarm rates. However its performance suffers during the detection of new emerging threats due to the limitation of known attack patterns.
- Anomaly detection (ADNIDS) uses the deviation from normal patterns to identify intrusions. Although ADNIDS produces high false positive alarms it is theoretically potential in the identification of novel attacks.

Objectives

Recurrent Neural Network model is used in a wide range of applications such as Intrusion Detection System. Recurrent Neural Networks has become famous due to the excellence performance and recurrent layers, uses previous inputs to compute the next output. RNNs were developed to work with sequence prediction problems.

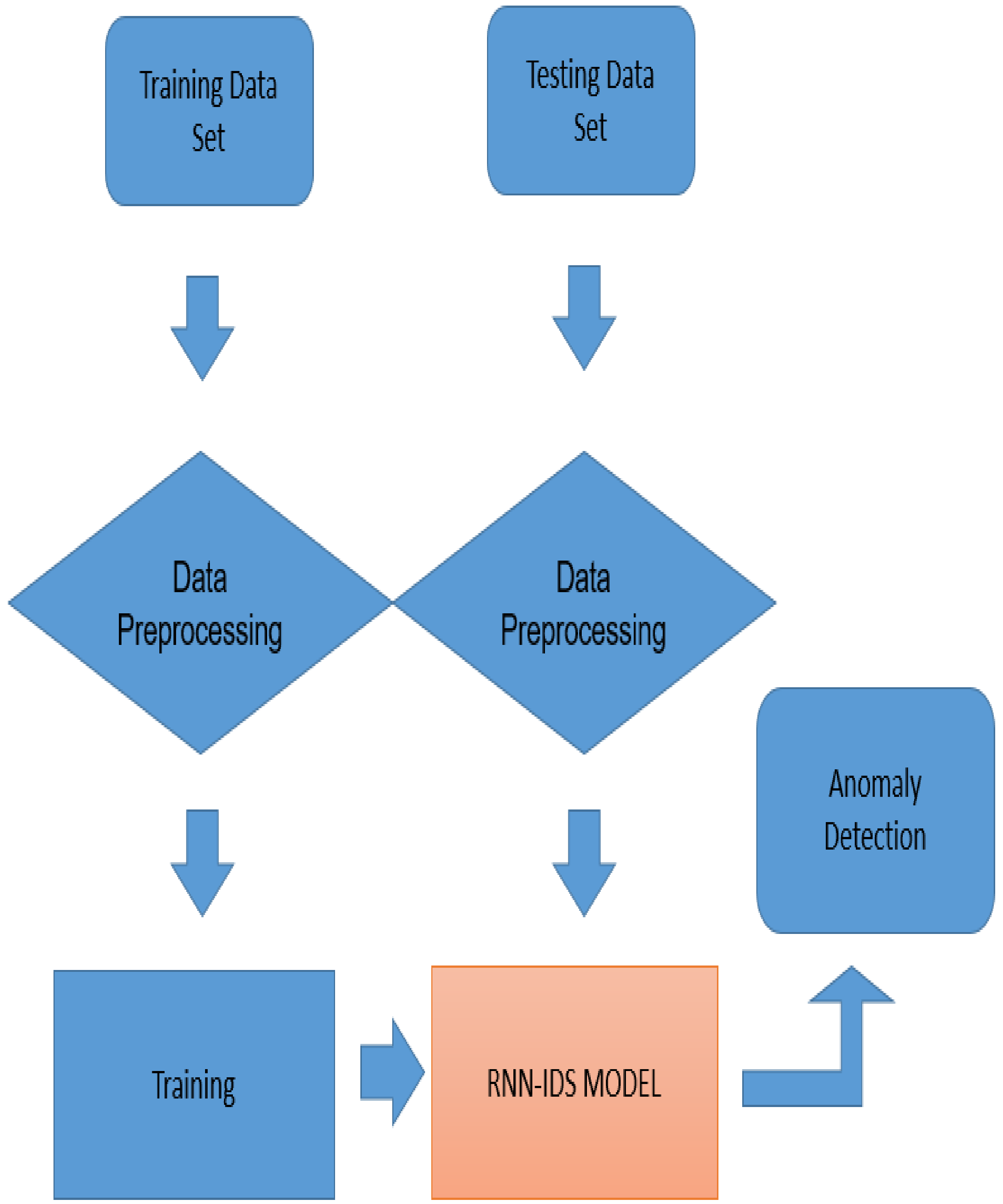
We use RNN for intrusion detection because network traffic is typically a sequential data. Our goal in this report is to improve the performance of Intrusion detection system using Recurrent Neural Network and reduce false positive alerts, also apply RNN with different variations such as LSTM, Simple RNN, and GRU.

Recurrent Neural Networks



Methodology

- Categorical data in the dataset is changed into model-understandable numerical data by label encoder.
- In our dataset protocol type, flags, services are categorical data. The problem here is, if we consider protocol type there are three protocol types(ftp, icmp, udp).so it will be numbered as 0,1 and 2 in any order. Since there are different numbers in the same column, the model will misunderstand that the data has some kind of order like 0<1. Hence hot encoding is performed.
- Preprocessed data is trained by RNN-IDS model.
- Using test data set accuracy is computed.



- Here NSLKDD and KDDcup have separate testing and training sets. Both data are preprocessed and trained by RNN-IDS model.

Testing Results

Experiments are performed on NSL-KDD and KDDCUP99 datasets. The testing results are presented in Table I, for NSLKDD dataset with binary classification. Here LSTM shows more accurate than Simple RNN and GRU shows more accuracy than the LSTM.

	SimpleRNN	LSTM	GRU
Classification rate	86.20%	81.64%	85.59%

The testing results are presented in Table 2, for KDDCUP dataset with binary classification. Here Simple RNN and GRU shows more accuracy than LSTM .

	SimpleRNN	LSTM	GRU
Classification rate	73.79%	75.85%	77.08%

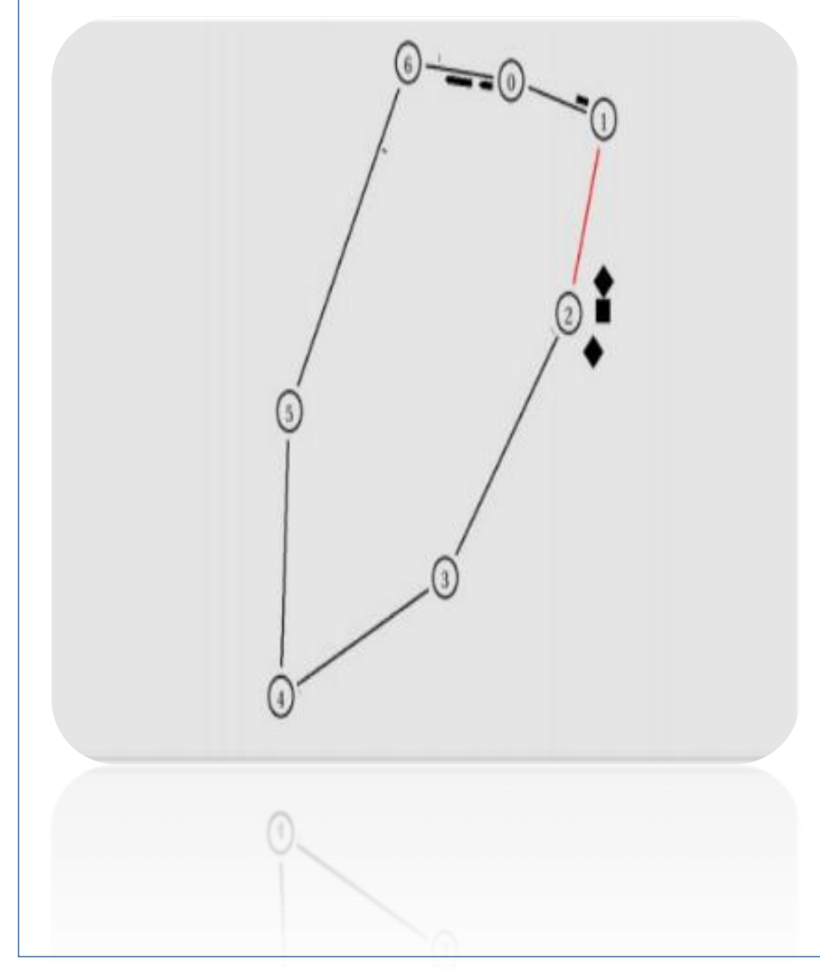
Conclusion and Discussion

In this work, different Deep Recurrent Neural Networks models are proposed to detect intrusions. The models have been implemented and tested on a benchmark dataset NSL-KDD.

- LSTM and GRU provides more accuracy than Simple RNN because they avoid vanishing gradient problem.
- Even Though ANN based model using KDD99 dataset gives high accuracy we can't consider it as a good measure because dataset has some redundancy problem.

In near future, we can configure the generated trace file in the simulation.

For the purpose of real data generation simulation set up for intrusion detection is needed. Here a simulation set up for malicious node in a wired network was carried out. The steps includes the following.



- Model a network.
- Configure the network according to research requirement.
- Add a malicious node in the network model.
- Generate trace file.

References

1. Chuanlong Yin , Yuefei Zhu, Jinlong Fei, and Xinzheng He, A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks,,pp- 2169-3536, November 7, 2017.
2. Ralf C. Staudemeyer, Applying long short-term memory recurrent neural networks to intrusion detection, SACJ No. 56, July 2015
3. P. Garcia-Teodoro, J. Diaz-Verdejo and E. Macia-Fernandez, G. and Vazquez. Anomaly-based network intrusion detection: Techniques, systems and challenges". Computers & security, vol. 28, no. 1-2, pp. 18{28, 2009. DOI http://dx.doi.org/10.1016/j.cose.2008.08.003.
4. Gozde Karatas , Onder Demir and Ozgur Koray Sahingoz,Deep Learning in Intrusion Detection Systems, DOI: 10.1109/IBIGDELFT.2018.8625278,December 2018.