Long Short-Term Memory based Operation Log Anomaly Detection

Vinayakumar R[1], K.P Soman[1] and Prabaharan Poornachandran[2]

[1]Centre for Computational Engineering and Networking (CEN), Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham,

Amrita University, India.

[2]Center for Cyber Security Systems and Networks, Amrita School of Engineering, Amritapuri, Amrita Vishwa Vidyapeetham,

Amrita University, India.

Outline

- Introduction
- Methodology
- Description of the data set and Results
- Summary
- Future Work
- References

Introduction

- A cloud infrastructure is of present interest, mostly adopted by many of the information technology (IT) firms instead of constructing their own monolithic or distributed IT infrastructures.
- Despite of the immense advantageous, predicting the system failures is of main important task, otherwise it might cause performance degradation of resources or entire downtime of resources inside cloud infrastructure.
- The system failures can arise from various sources such as software defects, hardware faults, attacks and misconfigurations.

Methodology

- The existing anomaly detection methods have largely focused on single point based [1]. They haven’t really taken the benefit of the past information in identifying the future event as either normal or anomalous.
- To overcome from these problems, we use long short-term memory (LSTM) [2]. LSTM is most prominent method for time-series data modeling that captures long-range temporal dependencies across time steps.

Contd.

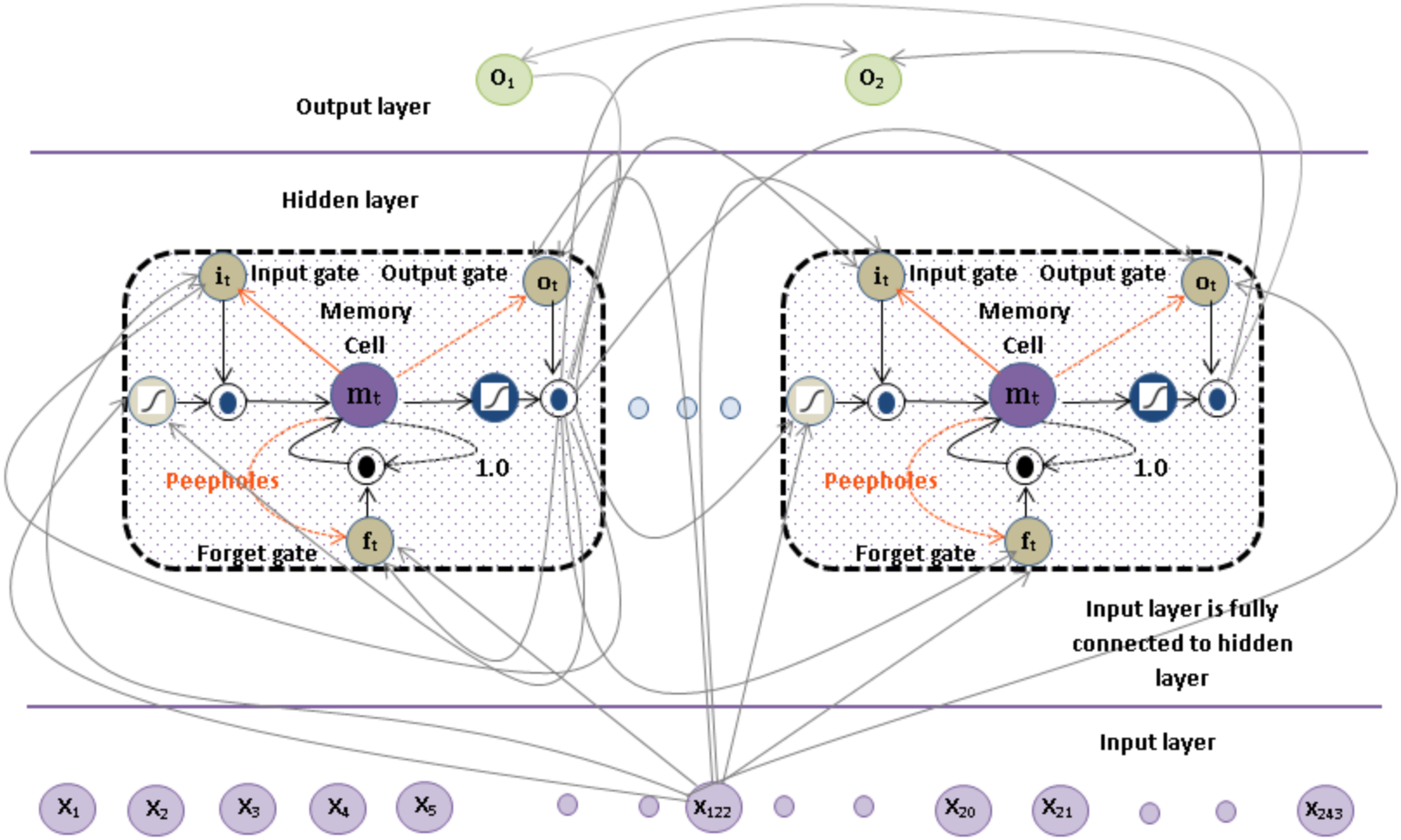

Figure 1. A subnet of LSTM network architecture including two memory blocks, each memory block has a single memory cell. Only fewer connections are shown.

Description of the data set and Results

UniteCloud is a resilient private Cloud infrastructure created in New Zealand Unitec Institute of Technology using OpenNebula for cloud orchestration and KVM for virtualization. The dataset is the operational data that captured from real-time running UniteCloud server with a sample period of 1-minute interval.

Table 1. Description of Data set

Total Samples	Total Features	Total Classes	Training	Testing
82,363	243	8	57,654	24,709

Contd.

Algorithm	Accuracy	Precision	Recall	F-measure
RNN 1 layer	0.933	1.00	0.917	0.957
RNN 2 layer	0.949	1.00	0.937	0.968
RNN 3 layer	0.981	1.00	0.977	0.988
LSTM 1 layer	0.935	0.997	0.922	0.958
LSTM 2 layer	0.983	1.00	0.979	0.989
LSTM 3 layer	0.994	1.00	0.993	0.996

Table 2. 5-fold cross-validation results of RNN and LSTM networks

Contd.

Overall accuracy	Class wise accuracy	Precision	Recall	Specificity
0.996	0.999	0.423	0.646	0.975

Table 3. Summary of test results using 3 layer stacked LSTM network with 32 memory blocks

Summary and Future work

- The LSTM architecture is proposed to detect and classify the anomalous events accurately in sensor log files.
- Stacked-LSTM (S-LSTM) has performed well in comparision to RNN. This is due to the fact that the S-LSTM has capability to learn long-range temporal dependencies quickly with sparse representations in the absence of preliminary knowledge on time order information.
- We lack in explaining the internal dynamics of LSTM network, this remained as one of significant direction towards future work.

References

[1] S. Hawkins, H. He, G. Williams, and R. Baxter, “Outlier detection using replicator neural networks,” in International Conference on Data Warehousing and Knowledge Discovery. Springer, 2002, pp. 170–180.

[2] Hochreiter, Sepp, and Jürgen Schmidhuber. "Long short-term memory." Neural computation 9.8 (1997): 1735-1780.