Malware Detection using Long-Short Term Memory Recurrent Neural Networks

Vinayakumar R
https://sites.google.com/site/vinayakumarr77/

Centre for Excellence in Computational Engineering and Networking
Amrita Vishwa Vidyapeetham, Coimbatore - 641112

7, October 2016

Outline

LSTM Architecture used in KDD data set

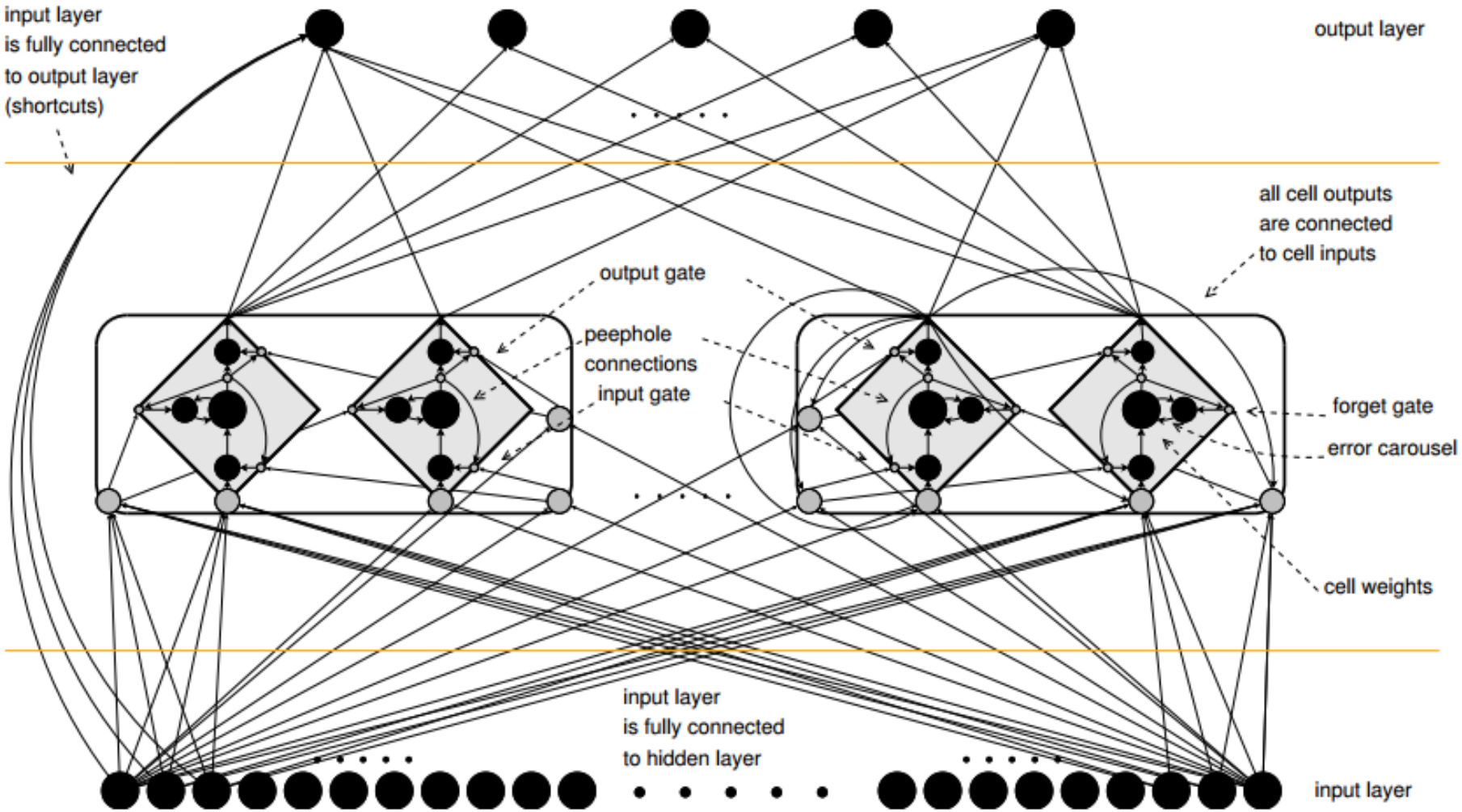

Figure: LSTM Architecture

Data Collection in mobile devices

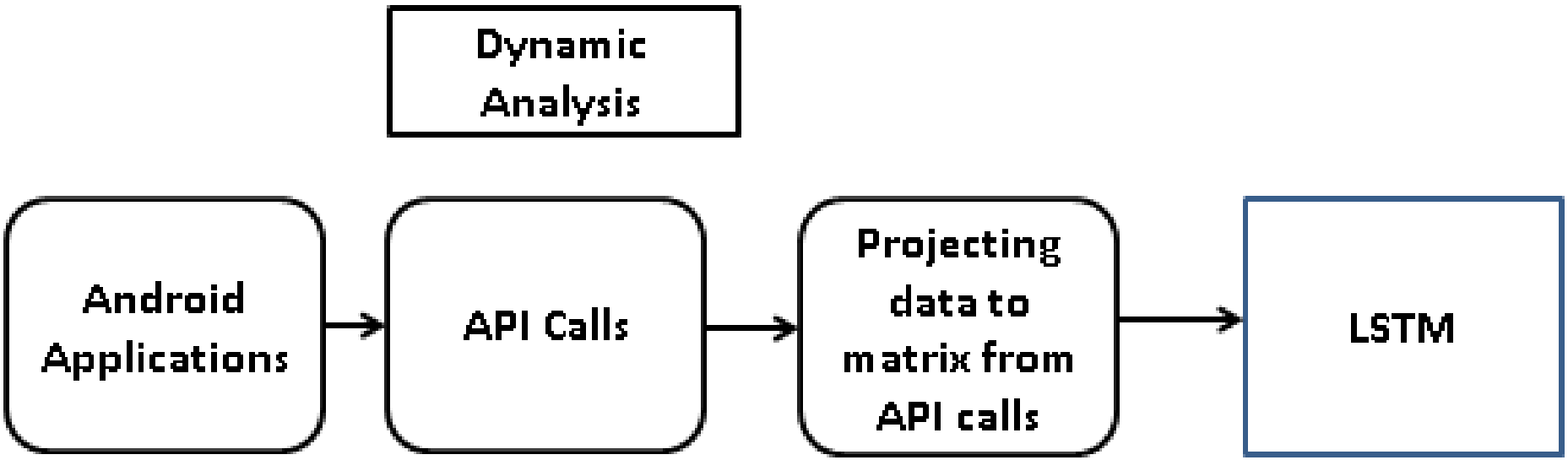

Figure: Data Collection in mobile devices

Data set information

- The data set has 42 features and 2 classes.
- Features: battIsCharging true,false,battVoltage numeric, battTemp numeric,cpuUsage numeric,networkTotalPackets numeric and so on
- Classes: 'Normal' or 'Attack'

Statistical Measures

Algorithm	Accuracy	Recall	Precision	F1-score	TPR	FPR
Ada boost	0.69384	0.434	0.743	0.548	0.43408	0.11212
K-nearest	0.67910	0.418	0.713	0.527	0.41785	0.12576
CART	0.68690	0.418	0.736	0.533	0.41785	0.11212
SVM	0.72333	0.479	0.792	0.597	0.47870	0.09394
ELM	0.70598	0.479	0.742	0.582	0.47870	0.12424
DBN	0.79271	0.805	0.735	0.769	0.80527	0.21667
DNN	0.84562	0.844	0.805	0.824	0.84381	0.15303
RNN	0.91067	0.931	0.869	0.899	0.93103	0.10455
LSTM	0.9982	1.000	0.997	0.998	0.99594	1.0000

Tutorials and Tools

Figure: Well documented and open source frameworks

References I


Ralf C. Staudemeyer, 'The importance of time: Modelling network intrusions with long short-term memory recurrent neural networks'. Ph.D thesis, University of the Western Cape, Cape Town / South Africa, 2012.


Sepp Hochreiter and Jrgen Schmidhuber. 1997. Long Short-Term Memory. Neural Comput. 9, 8 (November 1997), 1735-1780. DOI=http://dx.doi.org/10.1162/neco.1997.9.8.1735


R. Pascanu, J. W. Stokes, H. Sanossian, M. Marinescu, and A. Thomas. Malware classification with recurrent networks. In ICASSP15, pages 19161920