Chapter 18
Evaluation of Recurrent Neural Network and its Variants for Intrusion Detection System (IDS)

R Vinayakumar
Amrita School of Engineering, Coimbatore, India

K.P. Soman
Amrita School of Engineering, Coimbatore, India

Prabaharan Poornachandran
Amrita School of Engineering, Amritapuri, India

ABSTRACT

This article describes how sequential data modeling is a relevant task in Cybersecurity. Sequences are attributed temporal characteristics either explicitly or implicitly. Recurrent neural networks (RNNs) are a subset of artificial neural networks (ANNs) which have appeared as a powerful, principle approach to learn dynamic temporal behaviors in an arbitrary length of large-scale sequence data. Furthermore, stacked recurrent neural networks (S-RNNs) have the potential to learn complex temporal behaviors quickly, including sparse representations. To leverage this, the authors model network traffic as a time series, particularly transmission control protocol / internet protocol (TCP/IP) packets in a predefined time range with a supervised learning method, using millions of known good and bad network connections. To find out the best architecture, the authors complete a comprehensive review of various RNN architectures with its network parameters and network structures. Ideally, as a test bed, they use the existing benchmark Defense Advanced Research Projects Agency / Knowledge Discovery and Data Mining (DARPA) / (KDD) Cup '99' intrusion detection (ID) contest data set to show the efficacy of these various RNN architectures. All the experiments of deep learning architectures are run up to 1000 epochs with a learning rate in the range [0.01-0.5] on a GPU-enabled TensorFlow and experiments of traditional machine learning algorithms are done using Scikit-learn. Experiments of families of RNN architecture achieved a low false positive rate in comparison to the traditional machine learning classifiers. The primary reason is that RNN architectures are able to store information for long-term dependencies over time-lags and to adjust with successive connection sequence information. In addition, the effectiveness of RNN architectures are shown for the UNSW-NB15 data set.

DOI: 10.4018/978-1-7998-0414-7.ch018

INTRODUCTION

Over the years, information and communication technologies (ICT) systems have been bringing fruitful benefits to the human activities. Most of the businesses, government, academic and other organizations activities largely rely on ICT systems. On the other side, cyber-attacks to the ICT systems continuously evolving due to the fact that computer systems have constantly evolving from a handful of monolithic computing systems to distributed computing systems. In addition, recent days even a novice user can capable to attack many malicious activities easily with the freely available existing advanced attack toolkits in internet. The various cyber-attacks and its techniques occurred from 2001 to 2013 is briefly outlined by (Vaidya, T. 2015). These issues demand the necessity of flexible and interpretable integrated network security solutions to the ICT systems.

There are various approaches exist to attack malicious activities, namely (1) static approaches: firewalls, encryption and decryption techniques of cryptography, software updates and many others and (2) dynamic approaches: anomaly and intrusion detection (ID). In that, ID system has become a prominent method by achieving a great success in identifying various kinds of complex and diverse malicious foreseen threats. ID has been actively studied area since from 1980's, a seminal work by (Anderson, J. P. 1980) on the computer security threat monitoring and surveillance. Mainly, ID is categorized into 2 types based on the network behavior and network type. One is network-based ID system (N-IDS): most commonly used in both academia and industries, it analyzes all the network traffic by looking inside the packet level information to find the suspicious activity, the second one is host-based ID system (H-IDS): focuses on the information of each particular system or host, heavily depends for data on the sources of log files such as sensors, system logs, software logs, and many more. Mostly, organizations use combination of both of them to get benefited largely in real-time IDS deployment. The experiments used in this work are devoted to N-IDS using openly available data sets, KDDCup '99' and UNSW-NB15.

Primarily, analysis and classification of network traffic data is done using misuse detection, anomaly detection and state full protocol analysis. Misuse detection detects known specific attacks patterns accurately based on the predefined static signatures and filters. This method typically relies on human inputs to create and update the signatures and filters continuously whenever a new attack happens. In contrast to misuse detection, anomaly detection follows heuristic approach that enables them to find the unknown or novel attack patterns. However, this may result in a high false positive rate in most cases. To reduce this, most organization uses the combination of both the static and heuristic approaches, usually termed as hybrid approach. A third most power full method is state full protocol analysis that follows the similar approach as anomaly detection to identify the deviations of protocol state by using vendor's predetermined specific standards and specifications; usually these are generally accepted benign network traffic. This has become potential method and widely being discussed due to the capability to act on the network layer, application layer and transport layer. However, most commercial N-IDSs that are built to date and exist in market have predominantly based on the basic statistical measures or threshold computing approaches that uses traffic parameters such as packet length, inter-arrival time, and flow size and so on to model the network traffic in a categorical time slot. However, this still limit the performance in detection of complex pattern due to its built on simple statistical measures that are computed from packet header and packet contents. Due to the advancement in mathematics has given a birth to the new field called self-learning systems (SLS). SLS's are one of the potential methods that overcome the aforementioned limitations by leveraging the machine learning (ML) mechanisms. ML mechanisms are particularly supervised learning algorithms that learn the network traffic events of normal