Deep Learning Framework for Cyber Attack Prediction

Literature Review (E1)

Research Methods

Date:

Supervisor:

Name:

Student ID:

Table of Contents

1. Introduction

“Cyberattack” is a hot topic in today’s digitalized world. Cyber technologies have opened new doors to organizations and people to digitize them with the latest technologies and ease their work. Unfortunately, this has opened opportunities for illegitimate users like hackers as well. Cyber attacks are increasing immensely and make a great loss to organizations. For example, cyber-attacks increased by 37% over the past month with COVID19 pandemic (Muncaster, 2020). According to Bloomberg, a cyber attack hit the U.S. Health Agency this month to steal national health data and to publish fake news(SteinJacobs, 2020). In January 2020, the Puerto Rico government lost $2.6 Million in a phishing scam(PRESS, 2020). These cyber-threats make monetary losses, loss of trust, harm to people and it directly affects the reputation of the companies.

There are a lot of cybersecurity tools out there to secure cyberspace. It is always a necessity to predict the attack in the early stages before it harms the organization. So that the companies can set up precautions to stop the attack. For example, Honeypots and network telescopes monitor unsolicited internet traffic to gather data related to cyberattacks in networks and to allocate defence tools to secure the network(Peng et al., 2016).

The subject of predicting cyber attacks and efficient models have reached a top research topic in the last few years. Different authors followed different approaches to predict cyberattacks while having advantages and disadvantages in their models in different situations. The current research path moving towards top-notch technologies like artificial intelligence, machine learning, deep learning and big data.

2. Literature Analysis

This section introduces the related work conducted in the past by different researchers. This section includes different approaches they used, their conclusions, findings and drawbacks.

The paper written by Ling, introduces a regression-based analytical model to predict cyber attacks in Honeynets. Honeynets are composed of multiple honeypots. The main purpose of conducting this study was to identify geospatial and temporal patterns in the cyber attacks and use the knowledge for future attack predictions. The authors introduced a vector autoregression(VAR) model for honeynets. This study used a dataset with 9 AWS virtual honeypot hosts. The paper well explained the ways to use VAR and BigVAR models in predictions. The researchers introduced a fractional integration methodology to calculate Large Range Memory- LRM in each host which helps to achieve concise modelling and high performance. Moreover, they found that the dependency among hosts does not improve prediction accuracy if honeypot hosts are not directly connected in the same network(Ling et al., 2019).

The research conducted by Peng(2019) about cyberattack rates used another approach to accurately predict cyber attacks. These authors have studied extreme value phenomenon exhibits in cyberattack rates. In short, extreme value phenomenon is the number of attacks against a system of interest per time unit. This value is very important when allocating defence resources by the defender to protect networks at the right time. The authors introduced a marked point process technique to model and predict these extreme cyber-attack rates. They have used Value-at-Risk(VaR) to measure the intensity of the attacks over a period of time by providing the probability of extreme cyber-attack rates with a certain confidence level. In addition to that, they have used the Point Over Threshold(POT) method to model the magnitude of extreme attack rates.

Autoregressive Conditional Duration(ACD) approach is used to describe the arrival of extreme attack rates. Final analysis results revealed that using ACD and Log_ACD give higher precision on prediction than the FARIMA and GANCH models(Peng et al., 2016).

ARIMA, FARIMA and GANCH models are the most common conventional statistical models used in cyber attack predictions using time series data. Autoregressive Integrated Moving Average - ARIMA model is used to analyse time-series data(CryerChan, n.d.). Generalized Autoregressive Conditional Heteroskedasticity - GANCH model used for more accurate predictions by accommodating extreme value data in a time series(CryerChan, n.d.). Fractionally Autoregressive Integrated Moving Average - FARIMA model used to predict the cyberattacks with long-range dependent data in a time series and this is an extended version of ARIMA(Fang et al., 2019).

When compared to the research conducted by Ling, this marked point process is used in predicting extreme attack rates in clusters and they can accommodate the dependence between the inter-exceedance. This model is highly capable with large and small datasets. However, the authors assumed that 1h time gap(optimal unit of time) for the prediction is enough for the defender to allocate defence tools to secure the network. But this paper does not explain the ways to determine the optimal unit of time for the predictions. It is the main future work to be done in this process. Moreover, in this approach, the data in the dataset need to be preprocessed before using it for predictions. For example honeypot/telescope dataset can include data created as results of misconfigurations of the servers(Peng et al., 2016).

Another approach of predicting cyber attack is studied by Daria in 2019. He conducted this research on industrial systems and used Kalman filters. Kalman filters are time series analytical models which can efficiently process, recursively filter and analyse datasets. This study was conducted on a Gasoil data set which was collected as sensor data in the Gasoil Heating Loop process. The authors have selected industrial systems

for the study because detecting and predicting cyber attacks in industrial systems are complicated due to high heterogeneity and low intelligent devices. The researchers calculated the prediction rates using mean square error and mean absolute deviation values and received a great result when compared with other models in industrial systems(Daria et al., 2019).

When compared with other models described above, the usage of Kalman filter has given a high strength to this approach. These filters can be used on both linear and non-linear processes and use filtering recursively. This approach can reduce memory storage problems as this approach does not require to know the history and this uses system states for system state forecasting. This feature allows the model to adapt new conditions effectively. In addition to that extended version of this approach can analyse multivariate time series and forecast cyber-attacks which most of the other models are unable to accomplish(Daria et al., 2019).

The study completed by Ghiyas Smith(2011) introduced a novel approach to predict time series data using machine learning concepts. The reviewed papers above were based on statistical approaches and this paper used new technologies to predict future events. This paper is not directly written to the cybersecurity field, but it is a very worthwhile approach to use in the cyberattack prediction.

This research presents a novel homogeneous neural network approach known as Generalized Regression Neural Network (GEFTS–GRNN) Ensemble to forecast the future based on time-series data. This model uses a dynamic nonlinear weighting system which consists of base GRNNs and a combiner GRNN. General regression neural network- GRNN is another neural network algorithm. The base-level GRNN receives different sets of datasets with different seasonal time series patterns as inputs and passes the output to another combiner GRNN. When GRNN itself works with multiple predictors it gives worst performances(GheyasSmith, 2009) but this issue is

fixed with this GEFTS–GRNN. This approach increases the accuracy of the prediction. Not only GRNN but also this model is a combination of several well-respected algorithms(GheyasSmith, 2011).

The comparison between other models showed that GEFTS–GRNN is more powerful and accurate. This model eliminated most of the drawbacks other models have like local optima, overfitting, dimension disasters which make the algorithms inefficient. The other models are inefficient and give low accuracy results with seasonal time series as most of them are based on global approximators. But the proposed GEFTS approach uses local approximators and works well with seasonal time series data. This model has increased its prediction accuracy by having multiple neural networks(GheyasSmith, 2011).

The major disadvantage of GEFTS is, the algorithms used in this approach are complex and need high computational power. Because of the complexities, the time to calculate the prediction is higher than other models. Furthermore, this approach needs to preprocess data before passing them to the input layers(GheyasSmith, 2011).

With the development of machine learning the researchers tend to use other new technologies like deep learning to these prediction approaches. One of the main studies conducted using deep neural networks is the introduction of BRNN-LSTM by Fang and his team(Fang et al., 2019). This study used a novel bi-directional recurrent neural network with long short term memory framework(BRNN-LSTM). The bi-directional recurrent neural network(RNN) is a feed-forward network which helps the network to train itself and increase the prediction accuracy with the frequency of usage. LSTM is in-memory states which are used to store memory status at different nodes and they help to increase the performance. The training process of RNN can cause gradient vanishing problems and LSTM are used to fix it. The whole framework uses statistical properties of cyberattack rates time-series data(Fang et al., 2019).

The accuracy measurement like present mean absolute deviation and mean absolute percentage error values achieved remarkably high prediction accuracy rate for BRNN-LSTM than other models. The data preprocessing step is avoided in the BRNN-LSTM framework and the selection of fitted values is calculated using an algorithm. Furthermore, the researchers conducted a comparison against other analytical approaches with this deep learning approach and found that the deep learning approach is more accurate and reduces error rates than other models(NAMINAMIN, 2018).

However, the authors found that this BRNN-LSMT framework had missed the observed values on some occasions and these occasions are not predictable. The authors assumed the prediction accuracy as sufficient throughout the paper but this can vary from different situations. So there is more to improve in this concept to maximize accuracy and performance.

3. Conclusion

According to the literature review conducted, the cybersecurity attack prediction can be done as illustrated in the below figure.

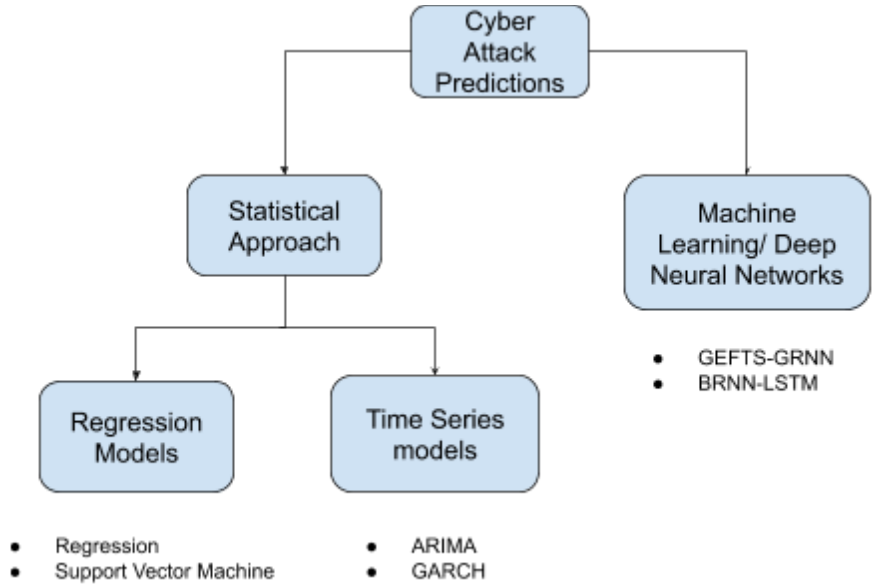

Figure 1: Cyber Attack prediction methodologies

According to the papers reviewed, there is a reasonable research gap to fill. The research is almost done for conventional statistical models and the new trend is moving towards deep learning technologies. The two papers reviewed related to machine learning and deep learning solved most of the problems the other models had with high prediction accuracy and performance. The framework introduced by Ghiyas Smith in 2011 found high computational costs and high complexities of the algorithms in its neural network. Moreover, the data needs to be preprocessed before passing it to the network. In 2019, Fang fixed all the research gaps GEFTS–GRNN had with Fang's BRNN-LSTM approach. In this approach, he used feedforward neural networks. Hence the preprocess stage is avoided. Furthermore, he introduced simple but highly accurate algorithms to predict the results. It minimizes the computational costs.

Fang's research(BRNN-LSTM) opens up opportunities for my research related to Deep Learning Framework for cyber attack prediction. BRNN-LSTM approach is mainly focused on predicting cyberattack rates. But this research paper does not consider predicting cyber attacks as a whole(denial of service attack, phishing attacks etc). BRNN-LSTM does not only rely on time series data. So Fang's approach will be the basement of my research topic. Even Though the neural network is the best solution for high accuracy and higher performance solutions, there are other advantages of using statistical approaches like Kalman filters and regression techniques in predictions. They have specific strengths the network can use with deep neural network technologies. These features can be implemented inside hidden layers of the network. Due to that the network can extract more information and can identify potential attacks efficiently. Thus the approach for Deep Learning Framework for cyber attack prediction will be a hybrid solution based on all the strength discussed above with minimised weaknesses.

References

Cryer, J. and Chan, K. (n.d.) *Time series analysis*. 2nd ed New York: Springer, p.92-102.

Daria, L., Dmitry, Z. and Anastasiia, Y. (2019) Predicting cyber attacks on industrial systems using the Kalman filter. *2019 Third World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*. *IEEE* [Online]. Available at: doi:10.1109/worlds4.2019.8904038 [Accessed: 24 March 2020].

Fang, X., Xu, M., Xu, S. and Zhao, P. (2019) A deep learning framework for predicting cyber attacks rates. *EURASIP Journal on Information Security*, 2019 (1). *Springer Science and Business Media LLC* [Online]. Available at: doi:10.1186/s13635-019-0090-6 [Accessed: 15 March 2020].

Gheyas, I. and Smith, L. (2009) A Neural Network Approach to Time Series Forecasting. *Proceedings of the World Congress on Engineering*, 2. [Online]. Available at: http://iaeng.org/publication/WCE2009/WCE2009_pp1292-1296.pdf [Accessed: 2 April 2020].

Gheyas, I. and Smith, L. (2011) A novel neural network ensemble architecture for time series forecasting. *Neurocomputing*, 74 (18), p.3855-3864. *Elsevier BV* [Online]. Available at: doi:10.1016/j.neucom.2011.08.005 [Accessed: 1 April 2020].

Ling, X., Rho, Y. and Ten, C. (2019) Predicting Global Trend of Cybersecurity on Continental Honeynets Using Vector Autoregression. *2019 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*. *IEEE* [Online]. Available at: doi:10.1109/isgteurope.2019.8905639 [Accessed: 4 April 2020].

Muncaster, P. (2020) Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites. *Infosecurity Magazine*. [Online]. Available at: https://www.infosecurity-magazine.com/news/cyberattacks-up-37-over-past-month/ [Accessed: 2 April 2020].

NAMIN, S. and NAMIN, A. (2018) *FORECASTING ECONOMIC AND FINANCIAL TIME SERIES: ARIMA VS. LSTM*. [Online]. Available at: doi:https://arxiv.org/pdf/1803.06386.pdf [Accessed: 21 March 2020].

Peng, C., Xu, M., Xu, S. and Hu, T. (2016) Modeling and predicting extreme cyber attack rates via marked point processes. *Journal of Applied Statistics*, 44 (14), p.2534-2563. *Informa UK Limited* [Online]. Available at: doi:10.1080/02664763.2016.1257590 [Accessed: 28 March 2020].

PRESS, A. (2020) Puerto Rico Loses $2.6 Million in Phishing Scam. *Courthousenews.com*. [Online]. Available at: https://www.courthousenews.com/puerto-rico-loses-2-6-million-in-phishing-scam/ [Accessed: 4 April 2020].

Stein, S. and Jacobs, J. (2020) Bloomberg - Are you a robot?. *Bloomberg.com*. [Online]. Available at: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response [Accessed: 3 April 2020].

Zhan, Z., Xu, M. and Xu, S. (2015) Predicting Cyber Attack Rates With Extreme Values. *IEEE Transactions on Information Forensics and Security*, 10 (8), p.1666-1677. *Institute of Electrical and Electronics Engineers (IEEE)* [Online]. Available at: doi:10.1109/tifs.2015.2422261 [Accessed: 19 March 2020].