Security Situation Prediction of Network Based on Lstm Neural Network

Liqiong Chen, Guoqing Fan, Kun Guo, Junyan Zhao

Security Situation Prediction of Network Based on Lstm Neural Network

Liqiong Chen[1], Guoqing Fan[1], Kun Guo[1], and Junyan Zhao[2]

[1] Department of Computer Science and Information Engineering Shanghai Institute of Technology, Shanghai 201400, China
lqchen@sit.edu.cn,1355744154@qq.com
[2] Department of Computer Science and Engineering East China University of Science and Technology, Shanghai 200237, China

Abstract. As an emerging technology that blocks network security threats, network security situation prediction is the key to defending against network security threats. In view of the single source of information and the lack of time attributes of the existing methods, we propose an optimal network security situation prediction model based on lstm neural network. We employ the stochastic gradient descent method as the minimum training loss to establish a network security situation prediction model, and give the model implementation algorithm pseudo code to further predict the future network security situation. The simulation experiments based on the data collected from Security Data dataset show that compared with other commonly used time series methods, the prediction accuracy of the model is higher and the overall situation of network security situation is more intuitively reflected, which provides a new solution for network security situation.

Keywords: Network security · Parallel processing · Situation awareness · Network security situation prediction model · Lstm network.

1 Introduction

As network systems evolve toward sharing, complexity, and scale, network intrusions become more complex and exist in various environments. The traditional way of network security mainly uses vulnerability scanning, intrusion detection and other protection technologies which has not been able to fully meet the increasingly updated network security needs [1]. Network security situational awareness technology emerged in this context. Network Security Situation Awareness (NSSA) is an emerging technology that studies how to acquire, understand, display, and predict network entities and build network security systems [2] [3].

The existing network security situation prediction methods mainly include Markov model [4], support vector machine [5] and other technologies. Although these technologies have improved the detection accuracy to a certain extent, they also have certain limitations. For example, they ignore the relevance of

data in a long sequence of time. In recent years, network security situation prediction methods based on deep learning have been proposed because of their better feature learning capabilities. However, although they improved the detection accuracy, they did not consider the characteristics of the result data after prediction.

In this paper, we propose an optimal network security situation prediction (ONS^{2}P) model for large-scale cyber-attacks with associated characteristics and time dimension. The main contributions of our work are listed as follows: (i)We employ the stochastic gradient descent method as the minimum sample training loss to optimize the parameters of the ONS^{2}P model established for the target, improving the accuracy of network security situation prediction. (ii) Simulation experiments show that compared with other commonly used time series methods, the prediction accuracy of the model is higher, and the overall situation of the network security situation is more intuitively reflected.

2 ONS^{2}P Algorithm

We design the ONS^{2}P algorithm based on the sltm network and convert a one-dimensional network security situation data set into a multi-dimensional network security situation data set before prediction. The Simple code is shown in Algorithm 1.

Algorithm 1 The ONS^{2}P prediction network security situation algorithm

Input: History attacked data set $D = x_1, x_2, x_n$
Output: predicted number of future network attacks K

1. Load the historical invalid data set and convert the data to floating point type float32.
2. Convert a list of network security postures into three columns of inputs *T-2*, *T-1*, T and a column of output *T+1*
3. MinMaxScalar achieves standardization of data.
4. Divide the data set into training set train X and forecast set test X
5. Transform the data into *[samples, time steps, features]* to construct the lstm model.
6. Establish ONS^{2}P model
   model.add(lstm(4, $input\_shape = (3, look\_back)$))
   model.add(Dense(1))
   model.compile($loss =' mean\_absolate\_error'$, $optimizer = sgd$)
   model.fit($trainX, trainY, epochs = 100, batch\_size = 1, verbose = 2$)
7. Use trained models to predict the number of attacks on the network K
8. Perform matrix operations on the predicted data, and output optimization.

In this paper, we also analyzed and optimized the predicted result data according to the predicted data characteristics: (1) When the hourly attack data

shows an increasing trend, the predicted value is a little larger; (2) When the hourly attack data is increasing When showing a decreasing trend, the predicted value is smaller.

If the current predicted value is greater than the predicted value of the previous time, then Xi is subtracted: $p_i^{'} = p_i + X_i(p_i - p_{i-1} >= 1)$. If the current predicted value is smaller than the predicted value of the previous time, then Xi is added: $p_i^{'} = p_i - X_i(p_i - p_{i-1} >= 1)$. The value of Xi is calculated from the average of the absolute values of the differences between the predicted data p and the real data x of multiple experiments: $X_i = \frac{\sum_{i=1}^{n}(|x_i - pi|)}{n}$,Where xi is the real data at time i, and pi is the predicted data at time i.

3 Experiment

We conduct experiments with the malicious program attack data collected by Honeynet organization to verify the validity and rationality of our method. In order to verify the performance of ONS^{2}P model, the two methods of Moving Average (MA) and Exponential Smoothing (ES) were used as reference models to do the same experiment.

We use the Root Mean Square Error (RMSE) and Mean Absolute Error (MAE) evaluation indicators to measure the accuracy of our method predictions, and the test results are shown in Table 1. The prediction results of the simulation experiment are shown in Figure 1.

Table 1: Comparison of experimental prediction results.

Model	ES	MA	LSTM	ONS^{2}P
Fitting RMSE	0.05	1.87	0.11	#
Prediction RMSE	0.13	0.63	0.10	0.10
Fitting MAE	0.08	0.14	0.09	#
Prediction MAE	0.12	0.13	0.08	0.06

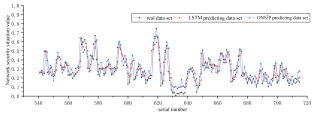


Fig. 2: Comparison of predictions before and after ONS^{2}P data optimization

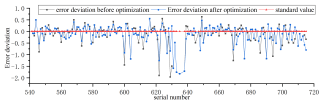
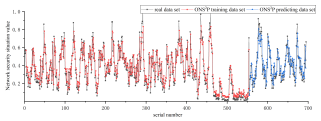
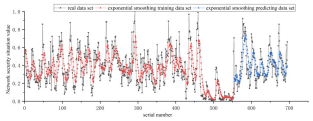


Fig. 3: Comparison of error deviation before and after ONS^{2}P model data optimization

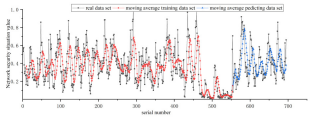
From the comparison data of Table 1 and Fig 1, the conclusion of this experiment can be drawn: from the overall prediction results, the ONS^{2}P model is



(a) Prediction results of ONS^{2}P simulation experiment



(b) Forecast results of exponential smoothing simulation experiment



(c) Prediction results of the moving average simulation experiment

Fig. 1: Results of prediction with different methods

more common than the commonly used time series prediction method. And the moving average method and the exponential smoothing method predict better. From the comparison results of the fitting error and prediction error provided in Table 1, it can be found that the commonly used time series prediction method moving average method and exponential smoothing method have large prediction errors, and the quantitative comparison results show that the ONS^{2}P model more accurately.

From the comparison data of Table 1, Fig 2 and Fig 3, the conclusion of this experiment can be drawn: the prediction value of the algorithm proposed in this paper is closer to the actual value than the prediction value of the lstm network. Therefore, it can be seen from the experimental results that the proposed optimization algorithm predicts the network situation better than the lstm neural network, and is more in line with the actual value.

4 Related works

Network security assessment is an important part of ensuring network security. Zhao, et al. [6] propose a grey Verhulst model or its inverse function to predict future risk values of the network system, and then correct the prediction accuracy based on multi-level residuals. In [7], authors proposed a quantitative evaluation method based on improved BP neural network to solve the problem of low efficiency and poor reliability of the existing network security situation assessment method. Lu [8] established a network security prediction model based on Grey Wolf Optimization (GWO) algorithm to optimize the support vector machine (SVM) parameters and solve the problem of SVM parameter optimization to improve the SVM prediction effect.

5 Conclusion

In this paper, we propose and establish a training model for the ONS^{2}P model. At the same time, we verify the accuracy of the model through experimental prediction data. The experimental results show that the ONS^{2}P model with the potential of learning long observation sequence is more accurate for network security situational awareness prediction, in order to further improve its prediction results. The accuracy of this paper is optimized for the prediction results. According to the experimental results, the error deviation after optimization is smaller, so a good optimization effect is obtained.

Acknowledgment This work is supported by the NSF of China under grants No. 61702334.

References

1. Caulfield T, Ioannidis C, Pym D. The U.S. Vulnerabilities Equities Process: An Economic Perspective, LNCS, volume 10575.pp. 131-150(2017).
2. Panteli M, Crossley P, Kirschen D, Sobajic D. Assessing the Impact of Insufficient Situation Awareness on Power System Operation. IEEE Transactions on Power Systems. 28. 2967-2977.(2013)
3. Tianfield H. Cyber Security Situational Awareness. Proceedings of 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData),782-787(2016).
4. Andrysiak Tomasz, Lukasz Saganowski, Miros?aw Maszewski, Adam. Detection of Network Attacks Using Hybrid ARIMA-GARCH Model. Advances in Dependability Engineering of Complex Systems, AISC, 582.1-12(2018).
5. Tai K S, Socher R, Manning C D. Improved Semantic Representations From Tree-Structured Long Short-Term Memory Networks. Computer Science, **5**(1).36(2015).
6. Guosheng Zhao, Huiqiang Wang, Jian Wang, and Linshan Shen. A Novel Situation Awareness Model for Network Systems' Security. In Proceedings of the 7th international conference on Computational Science, 1077-1084(2017).
7. Gangsong Dong, Wencui Li, Shiwen Wang, Xiaoyun Zhang, JiZhao Lu, Xiong Li. The Assessment Method of Network Security Situation Based on Improved BP Neural Network. Non-seismic and Non-conventional Exploration Methods for Oil and Gas in Cuba.67-76(2020).
8. Hongxia Lu, Guidong Zhang, Yongjun Shen. Cyber Security Situation Prediction Model Based on GWO-SVM. Innovative Mobile and Internet Services in Ubiquitous Computing, 162-171(2020).