Adversarial Attacks on Deep Neural Networks for Time Series Prediction

Aidong Xu*
Electric Power Research Institute, CSG, Guangzhou, China.Guangdong Provincial Key Laboratory of Power System Network Security, Guangzhou, China.

Xuechun Wang
School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China.

Yunan Zhang
Electric Power Research Institute, CSG, Guangzhou, China.Guangdong Provincial Key Laboratory of Power System Network Security, Guangzhou, China.

Tao Wu
School of Cybersecurity and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, China.

Xingping Xian
School of Cybersecurity and Information Law, Chongqing University of Posts and Telecommunications, Chongqing, China.

ABSTRACT

Time series data is widespread in real-world scenarios. To recover and infer missing information in practical domains, such as stock price monitoring, electricity load forecasting, traffic flows analysis, climate trend prediction, etc., the problem of time series prediction has been widely studied as a classical research topic in data mining. Over the past decade, deep learning architectures are introduced as a vital part of the next generation of time series prediction models. However, recent studies showed that deep learning models are vulnerable to adversarial attacks. In this paper, we study the adversarial attacks on the time series prediction models prospectively. We propose an attack strategy to generate adversarial samples by adding imperceptible perturbed data to the original time series with the goal of reducing the accuracy of time series prediction models. Specifically, the perturbation-based adversarial example generation algorithm is proposed using gradient information of time series prediction model. Moreover, adversarial examples should be imperceptible to humans. To address the challenge, we craft adversarial samples based on importance measuring to perturb the original data locally. We evaluate our attacks on state-of-the-art time series prediction models using three time series datasets. Our results demonstrate that our attacks can effectively evade the time series prediction models, and the adversarial attacks mechanisms can be used as robustness metric for constructing robust time series prediction models.

CCS CONCEPTS

• **Security and privacy**;

*Email addresses:xuad@csg.cn

ICICSE 2021, July 09–11, 2021, Guilin, China

ACM ISBN 978-1-4503-8495-7/21/07…$15.00
https://doi.org/10.1145/3485314.3485316

KEYWORDS

Time series data, Time series prediction, Adversarial attacks, Adversarial samples

ACM Reference Format:
Aidong Xu, Xuechun Wang, Yunan Zhang, Tao Wu, and Xingping Xian. 2021. Adversarial Attacks on Deep Neural Networks for Time Series Prediction. In *2021 10th International Conference on Internet Computing for Science and Engineering (ICICSE 2021), July 09–11, 2021, Guilin, China.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3485314.3485316

1 INTRODUCTION

Time series data refers to a series of statistical observations arranged in chronological order [1]. Time series data often arise when monitoring industrial processes or tracking corporate business metrics, such as stock price, electricity load, traffic flows, climate trend, etc. Time series analysis has been the subject of numerous research and development attempts in data mining [2], which help us get an understanding of the underlying forces and structure (such as autocorrelation, trend or seasonal variation) that produced the observed data. The problem of time series prediction is the use of a model to predict future values by analyzing the previously observed values and making an analogy or extension based on the development process, direction and trends reflected in the time series. Time series prediction has a wide variety of applications, such as predicting the weather in the next few days [3], forecasting traffic congestion [4], determining the electricity amount of power plants [5], detecting anomalous energy usage [6], etc.

The prediction of time series is to forecast the future by analyzing the time series and making an analogy or extension based on the development process, direction and trends reflected in the time series. There are many studies on time series, which attempt to develop better time series prediction models for different application scenarios in order to explore the underlying patterns of the data and the value that the data implies. Specifically, many traditional models have been proposed for time series prediction, such as autoregressive (AR) [7], exponential smoothing [8] and structural time series models [9]. Recently, because of the increases in data volume and computing resources, the research about time

series prediction is basically based on deep learning, where deep neural network models capture and exploit dynamic correlations between multiple variables, as well as consider a mixture of short and long-term repetitive patterns, which makes model predictions more accurately.

Deep neural network models enable time series prediction tasks to be completed with high accuracy, but recent studies have shown that models based on deep neural networks are vulnerable to adversarial attacks. Adversarial attacks seeks to find small and imperceptible perturbation and generate adversarial examples, resulting in an incorrect answer with high confidence. In 2013, Szegedy et al. [10] proposed the concept of adversarial attacks and initially applied adversarial samples to computer vision field. Kurakin et al. [11] found that adversarial samples generated by printing and photography can trick image recognition programs. Sharif et al. [12] proposed an attack method that allows an attacker to evade face recognition system. Eykholt et al. [13] demonstrated that an attacker can confuse an automated driving system by perturbing traffic signs. Xie et al. [14] generate an adversarial perturbation to give wrong prediction on all the output labels of the model, in order to fool either semantic segmentation or object detection models. Moreover, adversarial examples also exist in graph-structured data and text data [15–17].

Compared with the increasing interests in studying attack and defense mechanisms on images, graphs and text data, only recently some pioneering research has been done on generating adversarial samples for time series classification models. Specifically, Fawaz et al. [18], considering the vulnerability of deep learning models to adversarial time series examples, proposed to add imperceptible noise to the original time series thereby reducing the classification model accuracy. Karim et al. [19] proposes to use an adversarial transformation network (ATN) to attack various time series classification models. However, time series prediction models have gained significant importance in the research community, but not much research has been done on generating adversarial samples for these models. In this paper, we study the adversarial attacks on the time series prediction models prospectively.

In this study, we investigate the problem of adversarial attacks on time series by adding imperceptible perturbation. The key of time series prediction of adversarial attacks depends on how to generate adversarial examples that are difficult to detect; in other words, the difference between the adversarial samples and the original data should be as small as possible. To this end, this paper proposes a global perturbation based adversarial sample generation algorithm using the gradient information of the time series prediction model. To further reduce the perturbation cost, we propose an importance measure for adversarial samples to discover the most effective adversarial samples for prediction models. The work of this paper provides an opportunity to evaluate the robustness of time series prediction models. We evaluate our attacks on three time series datasets, and the results demonstrate that the attacks can effectively evade the time series prediction models.

2 PROBLEM DEFINITION AND FRAMEWORK

2.1 Problem Definition

Definition 1 (Time Series). $X = [x_1; x_2; \cdot s; x_T]$ is an ordered set of real values and the corresponding target series $Y = [y_1; y_2; \cdot s; y_T]$ where $x_i, y_i \in R^n$, n is the feature dimension, while T is the length of X.

Definition 2 (Time series prediction). To predict y_{T+h} where h is the desirable horizon ahead of the current time stamp. In the most of cases, the horizon of the forecasting task is chosen according to the demands of the environmental settings.

Definition 3 (Adversarial time series). Given a time series $X = [x_1; x_2; \cdot s; x_T]$, the attacker generates adversarial examples and construct an adversarial time series $\widehat{X} = [\widehat{x}_1; \widehat{x}_2; \cdot s; \widehat{x}_T]$, $\widehat{X} = X + \eta$ denotes the adversarial instance, where η represents the perturbation added to X. Additionally, on adversarial time series $\widehat{X}$, time series prediction model performs significantly worse.

Definition 4 (Time series prediction adversarial attacks). As we know, the accuracy of predictive models may decrease as perturbed data increases or directly changes the data distribution, but given the cost of data regulation and the added perturbation cannot be detected, the number of data manipulation should be reduced and minimized the distance between the perturbation time series and the original series. The process of minimizing the distance can be regarded as a constrained optimization problem, as defined in equation 1.

$$min||\widehat{X} - X|| \quad s.t.\ Y = f(X), \widehat{Y} = f(\widehat{X}) \tag{1}$$

2.2 Framework

Time series prediction models adversarial attacks are caused by well-designed adversarial sequences, which are designed to fool time series predictions methods. Given a time signal over a period of time, the time series prediction model can accurately predict the direction of future trends. The gradient attack-based approach generates adversarial samples to perturb the original time series and makes them mispredicted. The adversarial time series should be nearly as imperceptible as the original time series. In this paper, we attempt to minimize the distance between two sequences by regulating the perturbation through a gradient attack-based method to suppress the time series prediction inference. The time series prediction adversarial attacks including three components: adversarial time series generator, adversarial attack and transferable attack.

3 GRADIENT-BASED ADVERSARIAL ATTACKS FOR TIME SERIES PREDICTION

In this section, we explain how to generate the adversarial time series based on the gradient information from Long- and Short-Term Time-series Network (LSTNet) model.

3.1 LSTNet Model for Time Series Prediction

LSTNet is a deep learning model for multivariate time series prediction. Its overall architecture composed of a convolutional layer, a recurrent layer, a recurrent-skip layer, and a fully connected layer.

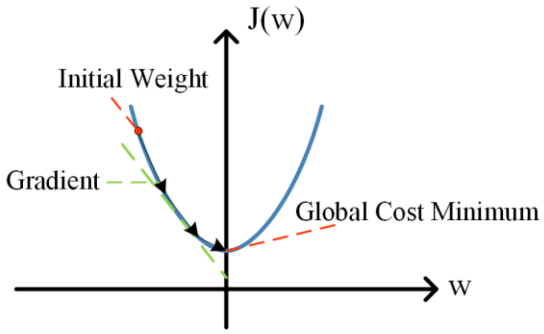

Figure 1: Gradient descent for the solving of LSTNet model.

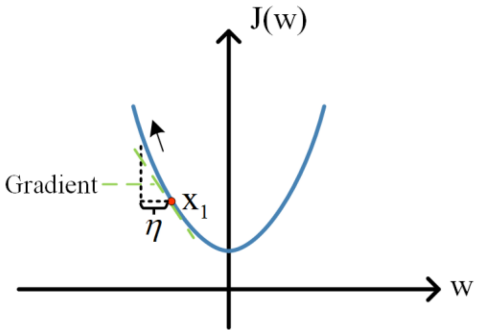

Figure 2: Gradient-based generation of adversarial samples.

Convolutional layer can extract local features for better performance. Recurrent layer can discover complex long-term dependencies in time series to acquire global patterns thus improving predictive performance. A new recurrent structure called recurrent-skip has been added to uncover very long-term dependency patterns and to make optimization easier by exploiting the periodicity of the time series. Lai et al. [20] proved that LSTNet works better than GRU/LSTM and has better robustness, so we use the LSTNet model as an attack target to verify that our method can attack the most state-of-the-art time series data prediction models.

3.2 Adversarial Time Series Generator

To acquire the generalization capability of the model, the LSTNet model is trained with a stochastic gradient descent optimization strategy, which uses the gradient to continuously update the weights so that the loss function is as small as possible, and the process is repeated until convergence and final weights are available. As shown in Figure 1, we assign the weights randomly, update the weight values and eventually converge to a global optimum solution.

This paper is inspired by the LSTNet model optimization strategy, which uses gradient information to update the weights in order to get an optimal solution to the model. To attack the LSTNet model, we can use gradient information to perturb the time series so that the error is as large as possible and the model outputs incorrect results. The optimization problem for adversarial attack is summarized as follows:

$$argmax J(\widehat{X}, Y) \quad s.t.\ ||\widehat{X} - X||_{\text{norm}} \leq \varepsilon \tag{2}$$

where J is the loss function and the LSTNet model uses ℓ_1 as the loss function, norm denotes the matrix norm, which can be equal to 2 or ∞. This constraint is used to control the amount of perturbation so that the distance between X and $\widehat{X}$ is as small as possible.

As shown in Figure 1, when training the model, we follow the opposite direction of the gradient to find the minimum value of the loss function. In order to generate adversarial time series sample to fool the time series prediction model, we can change the direction of gradient updating. Specifically, as shown in Figure 2, at the point x_1, we follow the direction of the gradient where the loss function is growing the fastest. In other words, we follow this direction that can find the maximum value of the loss function.

As shown in equation 3 and 4, $W \cdot \eta$ is the linear accumulation of noise. When the weights of the linear transformation are in the same or opposite direction as the perturbation, the value of $W \cdot \eta$ is either maximized or minimized, causing the output to exceed the normal range and making the model f prediction incorrect.

$$\widehat{X} = X + \eta \tag{3}$$

$$f(W \cdot \widehat{X}) = f(W \cdot X + W \cdot \eta) \tag{4}$$

According to the above discussion, the details for adversarial time series generator are summarized in Algorithm 1.

Algorithm 1 Adversarial time series generator

Input: Original time series X, Original time series label Y, number of iterations K, amount of maximum perturbation ε, $\alpha = \varepsilon/\varepsilon KK$;
Output: Adversarial time series $\widehat{X}$, learned time series prediction model f;
1: Train the time series prediction model on X and Y;
2: **for** $i = 1toK$ **do**
3: Calculate the gradient $\nabla_X J(X, Y)$;
4: $\eta = \alpha \cdot sign(\nabla_X J(X, Y))$;
5: $\widehat{X} = X + \eta$;
6: **end for**
7: Return the adversarial time series $\widehat{X}$ based on global perturbations, learned time series prediction model f.

3.3 Adversarial Sample Importance Measure

Inspired by feature importance ranking [21], where the contribution of individual input features to the model performance is measured to solve the optimal subset of features, we assume the adversarial samples have different contributions to the impact on model performance. Thus, the model can be fooled by perturbing only the important adversarial samples while reducing the difference between the perturbed time series and the original time series on the basis of Algorithm 1. Specifically, this paper proposes a method to measure the importance of the adversarial sample. The distance between $\widehat{y}_i$ and y_i is calculated, and the larger the distance, the greater the contribution of the adversarial sample $\widehat{x}_i$, which illustrates the importance of adversarial sample $\widehat{x}_i$. Finally, based on the perturbation proportion P, we select the top P most important samples to replace the corresponding samples in the original time

series to obtain the local perturbation-based adversarial time series. The details of local perturbation based adversarial time series generator are shown in Algorithm 2.

Algorithm 2 Local perturbation based adversarial time series generator

Input: Original time series X and T is the length of X, original time series label Y, adversarial time series $\widehat{X}$, time series prediction model f, perturbation proportion P;
Output: Adversarial time series $\widehat{X}'$;
1: Calculate the predictive value $\widehat{Y}$ on global adversarial sample $\widehat{X}$, $\widehat{Y} = f(\widehat{X})$;
2: **for** $i = 1 to T$ **do**
3: Calculate the distance between $\widehat{y}_i$ and y_i;
4: **end for**
5: Rank the distance between $\widehat{y}_i$ and y_i in descending order;
6: Select the top P adversarial samples $\widehat{x}_i$ according to the ranking results;
7: Replace the selected P samples $\widehat{x}_i$ with the corresponding samples x_i in the original time series to obtain the locally perturbed adversarial samples $\widehat{X}'$;
8: Return the adversarial time series $\widehat{X}'$ based on global perturbations.

According to the above, this paper proposes an adversarial time series generation algorithm based on global perturbations and an adversarial time series generation algorithm based on local perturbations, and we can choose the algorithm according to demand. When we have a time constraint, we choose Algorithm 1, which has better time-sensitivity. When we have more tolerance for time and desire the adversarial samples to be more imperceptible to human, we can choose Algorithm 2.

4 EXPERIMENTS

In this section, extensive experiments are conducted to verify the effectiveness, applicability and transferability of the proposed attack algorithms. We present the experiments results using different predictive models and multiple evaluation metrics on different real-world datasets.

4.1 Experiments Setup

Datasets. This paper uses three publicly available power datasets Electricity [22],Solar [23] and Household power consumption [24], which are divided into training set, validation set, and test set at scales of 0.6, 0.2, and 0.2, respectively.

Time Series Prediction Methods. To demonstrate that our attack methods are applicable to different models and that the generated adversarial samples can be transferred over different models, we present Convolutional Neural Network (CNN), Recurrent Neural Network (RNN) and Multi-Head Attention Network (MHANet) [25] as state-of-the-art time series methods for evaluation.

Metrics. This paper uses three evaluation metrics that are widely used in prediction tasks: Root Relative Squared Error (RSE), Relative Absolute Error (RAE), and Empirical Correlation Coefficient (CORR). In the prediction task, lower error values and higher correlation coefficients indicate better prediction performance. However, our goal in attacking the predictive model is to make its predictions inaccurate, that is to say, the larger the error value and the lower the correlation coefficient means that our attack is effective. We also use a Frobenius norm (F-Norm) to illustrate the distance between the adversarial sample and the original data. In the experiments of this paper, the distance between the adversarial time series sample and the original time series is quantified using F-Norm, and the distance between the adversarial sample and the original time series should be as small as possible.

Parameter Setting. The parameter ε in Algorithm 1 represents the total amount of perturbations in the adversarial time series samples. If we set it very large (meaning the perturbation is large), it will make the time series prediction model forecast value very worse. Although it achieves our goal of fooling the predictive model, the amount of perturbations is so large that they are easily identified and removed as noise, and the availability of the data is also reduced. The purpose of this paper is to add imperceptible perturbations to fool the predictive model, so the value of ε should not be set too large. Here, we set the ε values to 0, 0.05, 0.1, 0.15, and 0.2 respectively to evaluate the performance of the methods extensively.

4.2 Effectiveness evaluation

We use three datasets, three evaluation metrics, and five parameter values for experimental validation of the proposed algorithm. Tables 1 shows the performance of adversarial attacks on LSTNet. When ε is equal to 0, we find that LSTNet predicts the original time series pretty well (low error and high correlation coefficient). As the value of ε gradually increases, we find that the error of the predicted values also increases and the correlation coefficient decreases.

4.3 Transferability evaluation

Transferable attack is an adversarial sample generated for a particular time series prediction model that is capable of tricking other time series prediction models. In this paper, the transferable attack is experimentally validated using the three datasets mentioned above and four time series prediction models with a perturbation parameter choice of 0.1. The selection of the perturbation parameter here is based on the above experimental results.

Figure 3, 4, 5 shows the transferability validation on three datasets, with four columns corresponding to the adversarial samples generated by the CNN, LSTNet, MHANet, and RNN models, respectively. The adversarial samples generated by the each of them are used to attack the other three models, and the attack effectiveness is illustrated by the three evaluation metrics of RSE, RAE, and CORR. For example, the first column of the figure shows the adversarial sample generated for the CNN, and after using this adversarial samples to attack the three models LSTNet, MHANet, and RNN, the error values RSE and RAE corresponding to each model increase and the correlation coefficient CORR decreases. It is worth noting that the adversarial samples generated for a specific model are more effective in attacking the target model than the other models.

Table 1: The effectiveness of adversarial attack against LSTNet

Datasets	Metrics	ε				
		0	0.05	0.10	0.15	0.20
Electricity	RSE	0.1020	0.8098	0.8502	0.8822	0.9583
	RAE	0.0581	0.4039	0.4460	0.4909	0.5562
	CORR	0.8712	0.0034	-0.0085	0.0021	0.0059
Solar	RSE	0.4309	1.7658	2.0727	2.2691	2.4294
	RAE	0.2447	1.8743	2.2089	2.4324	2.6405
	CORR	0.9090	0.0081	-0.0028	-0.0067	0.0101
Household	RSE	0.4960	0.8064	0.9039	1.0157	1.1304
	RAE	0.3209	0.5707	0.6412	0.7335	0.8216
	CORR	0.6236	0.0030	-0.0122	-0.0317	0.0050

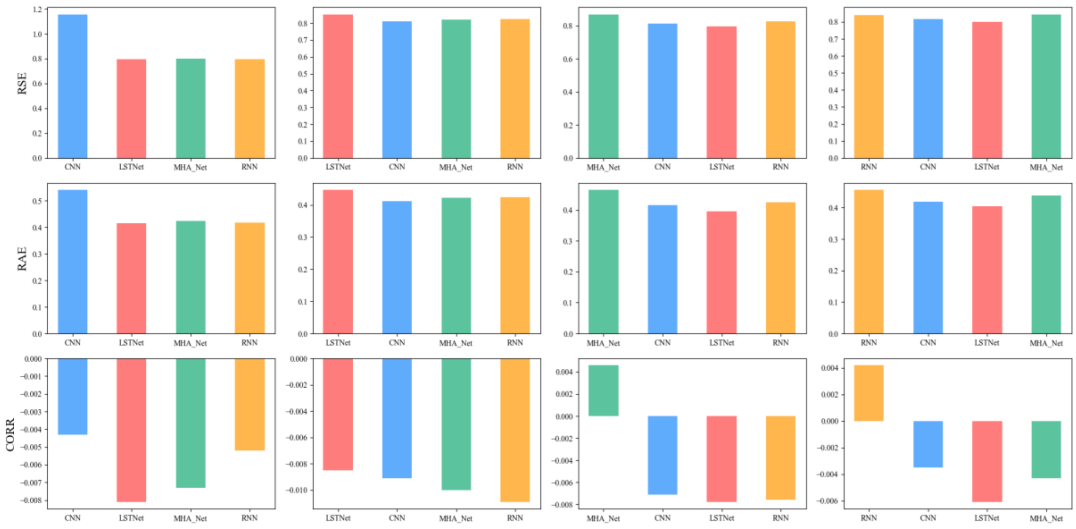

Figure 3: Transferability validation on the Electricity Dataset

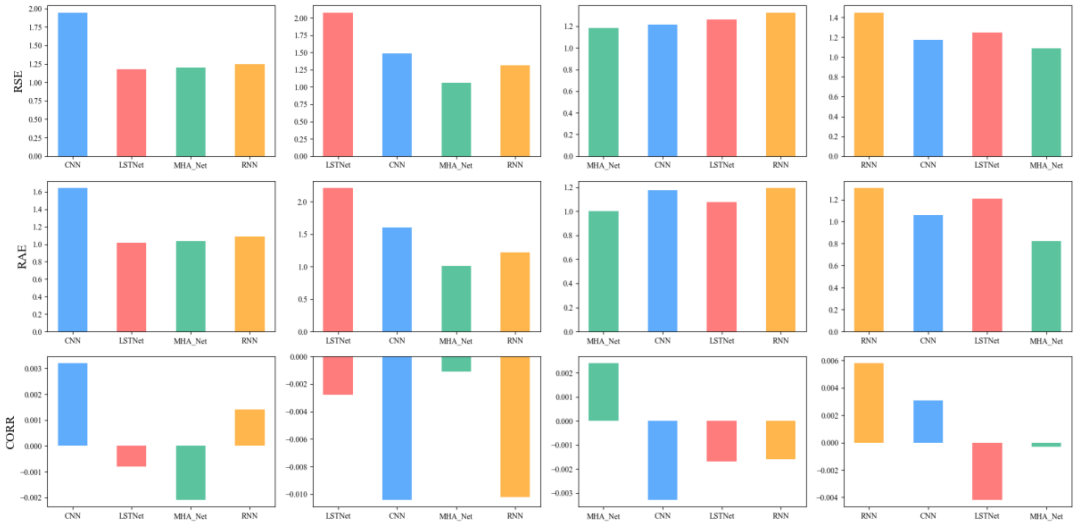

Figure 4: Transferability validation on the Solar Dataset

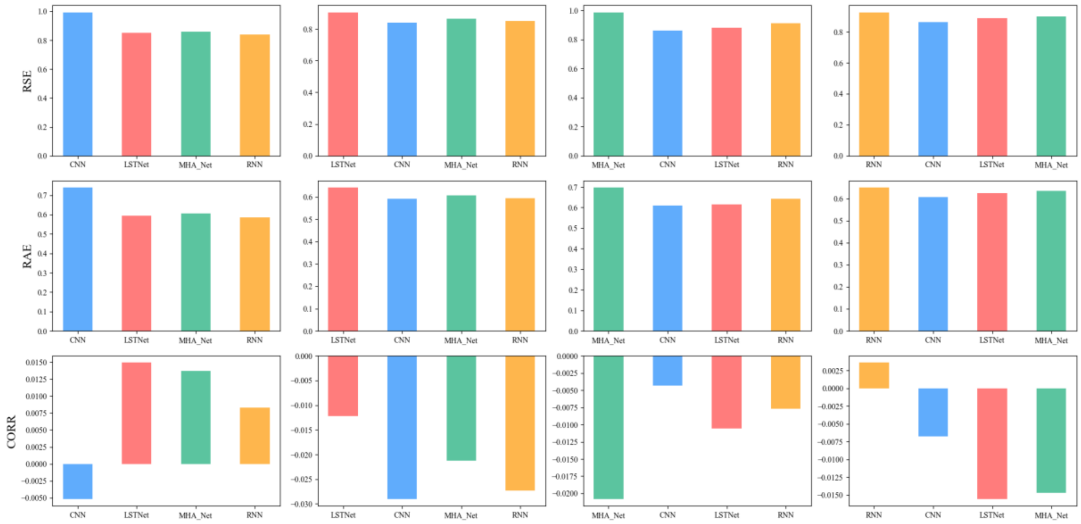

Figure 5: Transferability validation on the Household Dataset

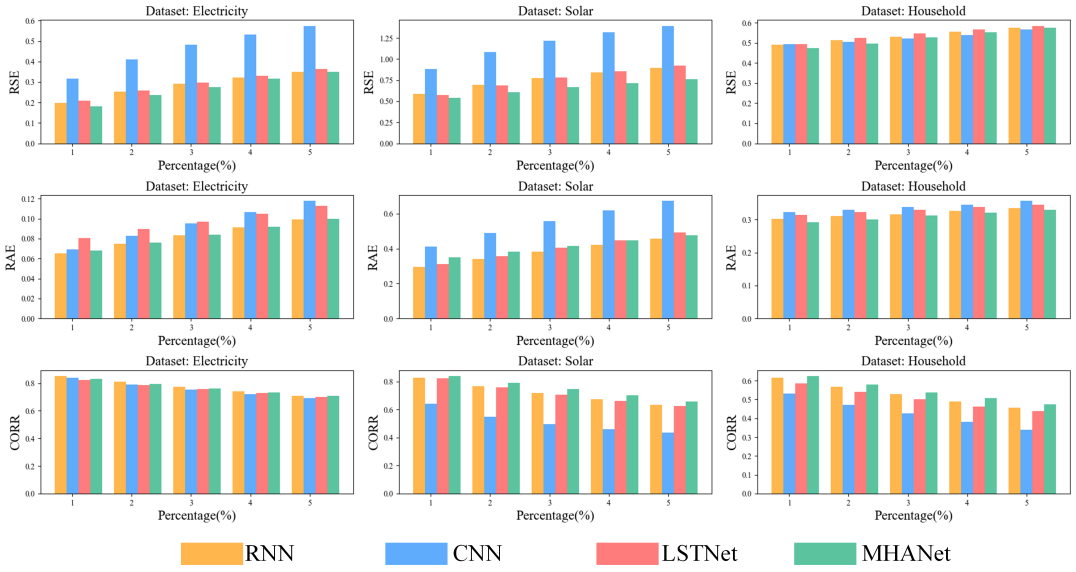

Figure 6: Performance of local perturbation-based adversarial attacks under various perturbation percentages.

4.4 Evaluation of the local perturbation based adversarial attacks

This subsection is an experimental validation of the local perturbation-based adversarial sample generation algorithm. Algorithm 2 local perturbation adversarial samples are obtained based on the global adversarial samples generated by Algorithm 1 after further selection. Specifically, we measure and rank the importance of each adversarial sample in the global sample, and select the top P% of adversarial samples to replace the original time series. The local perturbation algorithm further reduces the difference between the adversarial samples and the original data, making it more difficult for the attacker to detect, and achieving a better attack effect with a very small perturbation cost.

Figure 6 shows the performance of the adversarial sample generation algorithm based on local perturbations on three data sets and four models. The horizontal coordinates indicate the perturbation percentage of Algorithm 2, and the vertical coordinates are the three evaluation metrics RSE, RAE, and CORR, respectively. With the increase of the perturbation percentage, RSE and RAE increase and CORR gradually decreases.

5 CONCLUSIONS AND DISCUSSION

This study focuses on the problem of adversarial attacks on time series prediction models. To the best of our knowledge, there is little research on the security of time series prediction models. It is significant to study the adversarial attacks on time series prediction models, not only for the security of time series prediction based intelligent systems, but also for the privacy protection of time series data. In this paper, we formulate the problem of adversarial attacks on time series prediction models and propose a global perturbation-based adversarial attack method for the current advanced time series prediction models.

In order to further reduce the difference between the adversarial sample and the original data and make the adversarial samples more imperceptible, this paper proposes an adversarial sample importance measure to identify the important samples. Extensive experiments demonstrate that the proposed adversarial attack methods are applicable to state-of-the-art deep learning based time series prediction models.

ACKNOWLEDGMENTS

This work is partially supported by National Key R&D Program of China under Grant No. 2018YFB0904900, 2018YFB0904905; Natural Science Foundation of Chongqing under Grant No. cstc2020jcyj-msxmX0804, National Natural Science Foundation of China under Grant No. 61802039, 61772098, 61772091.

REFERENCES

[1] Esling P, Agon C. 2012. Time-series data mining. ACM Computing Surveys (CSUR), 45, 1 (December 2012), 1-34. https://doi.org/10.1145/2379776.2379788.

[2] Fu T. 2011. A review on time series data mining. Engineering Applications of Artificial Intelligence, 24, 1 (February 2011), 164-181. https://doi.org/10.1016/j.engappai.2010.09.007.

[3] Grover A, Kapoor A, Horvitz E. 2015. A deep hybrid model for weather forecasting. In Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. Association for Computing Machinery, New York, NY, USA, 379-386. https://doi.org/10.1145/2783258.2783275.

[4] Koesdwiady A, Soua R, Karray F. 2016. Improving traffic flow prediction with weather information in connected cars: A deep learning approach. IEEE Transactions on Vehicular Technology, 65, 12 (June 2016), 9508-9517. https://doi:10.1109/TVT.2016.2585575.

[5] Bedi J, Toshniwal D. 2019. Deep learning framework to forecast electricity demand. Applied energy, 238, (March 2019), 1312-1326. https://doi.org/10.1016/j.apenergy.2019.01.113.

[6] Zheng Z, Yang Y, Niu X, *et al.* 2018. Wide and deep convolutional neural networks for electricity-theft detection to secure smart grids. IEEE Transactions on Industrial Informatics, 14, 4 (April 2018), 1606-1615. https://doi.org/10.1109/TII.2017.2785963.

[7] Box G E P, Jenkins G M, Reinsel G C, *et al.* 2015. Time series analysis: forecasting and control. John Wiley & Sons.

[8] Gardner Jr E S. 1985. Exponential smoothing: The state of the art. Journal of forecasting, 4, 1 (March 1985), 1-28. https://doi.org/10.1002/for.3980040103.

[9] Turner L W, Witt S F. 2001. Forecasting tourism using univariate and multivariate structural time series models. Tourism Economics, 7, 2 (June 2001), 135-147. https://doi.org/10.5367/000000001101297775.

[10] C. Szegedy, W. Zaremba, I. Sutskever, J. Bruna, D. Erhan, I. Goodfellow, R. Fergus. 2013. Intriguing properties of neural networks. arXiv preprint arXiv:1312.6199 (December 2013).

[11] A. Kurakin, I. Goodfellow, S. Bengio. 2017. Adversarial examples in the physical world, arXiv preprint arXiv:1607.02533 (February 2017).

[12] M. Sharif, S. Bhagavatula, L. Bauer, M. K. Reiter. 2016. Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition. In Proceedings of the 2016 acm sigsac conference on computer and communications security. Association for Computing Machinery, New York, NY, USA , 1528–1540. https://doi.org/10.1145/2976749.2978392.

[13] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, D. Song. 2018. Robust physical-world attacks on deep learning visual classification. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. IEEE, Salt Lake City, UT, USA, 1625–1634. https://doi.org/10.1109/CVPR.2018.00175.

[14] C. Xie, J. Wang, Z. Zhang, Y. Zhou, L. Xie, A. Yuille. 2017. Adversarial examples for semantic segmentation and object detection. In Proceedings of the IEEE International Conference on Computer Vision. IEEE, Venice, Italy, 1369–1378. https://doi.org/ 10.1109/ICCV.2017.153.

[15] H. Xu, Y. Ma, H.-C. Liu, D. Deb, H. Liu, J.-L. Tang, A. K. Jain. 2020. Adversarial attacks and defenses in images, graphs and text: A review. International Journal of Automation and Computing. 17, 2(March 2020), 151–178. https://doi.org/10.1007/s11633-019-1211-x.

[16] D. Zugner, A. Akbarnejad, S. G. unnemann. Adversarial attacks on neural networks for graph data. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. IEEE, Günnemann, Stephan, 2847–2856. https://doi.org/10.1145/3219819.3220078.

[17] J. Ebrahimi, A. Rao, D. Lowd, D. Dou. 2017. Hotflip: White-box adversarial examples for text classification, arXiv preprint arXiv:1712.06751(May 2018).

[18] H. I. Fawaz, G. Forestier, J. Weber, L. Idoumghar, P. A. Muller. Adversarial attacks on deep neural networks for time series classification. In 2019 International Joint Conference on Neural Networks (IJCNN). IEEE, Budapest, Hungary, 1–8. https://doi.org/10.1109/IJCNN.2019.8851936.

[19] F. Karim, S. Majumdar, H. Darabi. 2020. Adversarial attacks on time series. IEEE Transactions on Pattern Analysis and Machine Intelligence (Early Access). https://doi.org/10.1109/TPAMI.2020.2986319.

[20] G. Lai, W.-C. Chang, Y. Yang, H. Liu. 2018. Modeling long-and short-term temporal patterns with deep neural networks. In the 41st International ACM SIGIR Conference on Research & Development in Information Retrieval. Association for Computing Machinery, New York, NY, USA, 95–104. https://doi.org/10.1145/3209978.3210006.

[21] Wojtas M, Chen K. 2020. Feature Importance Ranking for Deep Learning. arXiv preprint arXiv:2010.08973 (October 2020).

[22] ElectricityLoadDiagrams20112014 Data Set. Retrieved from https://archive.ics.uci.edu/ml/datasets/ElectricityLoadDiagrams20112014.

[23] Solar Power Data for Integration Studies. Retrieved from https://www.nrel.gov/grid/solar-power-data.html.

[24] Individual household electric power consumption Data Set. Retrieved from https://archive.ics.uci.edu/ml/datasets/individual+household+ electric+power+consumption

[25] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, I. Polosukhin. 2017. Attention is all you need. In Proceedings of the 31st International Conference on Neural Information Processing Systems. Curran Associates Inc., Red Hook, NY, USA, 5998–6008. https://doi.org/10.1105/1706.03762.