Prediction Methods for Energy Internet Security Situation Based on Hybrid Neural Network

Dongmei Liu¹, Jie Cheng¹, Zilong Yuan², Chan Wang¹, Xingjie Huang¹, Hongshan Yin¹, Nan Lin¹ and Haihang Niu³

¹Information and Communication Branch of State Grid Corporation of China, Xicheng District, Beijing, 100032, China
²College of science, Beijing Information Science and Technology University, Haidian District, Beijing, 100192, China
³Institute of Software Chinese Academy of Sciences, Haidian District, Beijing, 100089, China

Corresponding author’s e-mail: 19900422@bistu.edu.cn

Abstract. Under the duplex framework of the rapid transformation of the conventional power grid to the energy Internet and the swift development of network attack technologies, the security and protection of the energy Internet are becoming increasingly precarious. The energy Internet attack prediction method has become a current research hotspot. The current research in this area is predominantly focused on security to protect and reduce losses, it is impossible to counter the attacks faced by the Energy Internet promptly, and there is a lack of online predictive security analysis methods and tools. Aiming at the shortcomings of traditional research and the current stage, this paper proposes an online prediction and analysis method of energy Internet security situation based on the combination of temporal convolutional neural network (TCN) and gated recurrent neural network (LSTM). This method which based on the security status data set can predict and analyse the region Energy Internet security, and the mean absolute error and mean squared error are 0.352 and 0.2714 respectively. The results show that the prediction performance of the algorithm has been improved, the stability is robust, and it can be applied to the energy Internet security situation prediction.

1. Introduction

Energy Internet can be defined as a comprehensive application of advanced power electronic technology, information technology, and intelligent management technology to interconnect a large number of energy nodes composed of distributed energy harvesting devices, distributed energy storage devices, and various types of loads to achieve bidirectional energy flow and peer-to-peer energy exchange and sharing network[1].

The main security risks and problems facing the Energy Internet are power generation system attacks[2], Phasor Measurement Units (PMU) attacks[3], state estimation attacks[4], blockade attacks[5], load redistribution Attacks[6], cyber-physical exchange attacks[7], distributed systems and user-side attacks[8], false data injection attacks[9], power market attacks[10], substation attacks[11], and traditional network attacks, etc., these threats seriously affects the security of the Energy Internet.
In 2010, Stuxnet, the first computer virus specifically aimed at industrial control systems, appeared [12]; in 2015, Ukraine's power network was hacked and damaged, and the BlackEnergy Trojan was maliciously implanted, resulting in huge losses in the country's social and economic production [4].

Literature [13] takes the power space of the cyber-physical system (cyber-physical system, CPS) as the main research object, and conducts a preliminary discussion on the propagation mechanism of network security risks in power CPS, and uses cellular automata to analyze power cps information. Physical security risk propagation is analyzed; this method can only block the propagation of failures and risks, avoid the expansion of losses, and cannot contain failures and risks in time. Literature [1] starts with the development trend of the energy-critical infrastructure itself, and analyzes the mechanism of the traditional and new security threats it faces; on this basis, it conducts in-depth research and analysis on the defense technology of energy-critical infrastructure. The analysis provides a good reference for energy-critical infrastructure network security defense. The literature [14] focuses on the information security of the global energy Internet, with the Ukrainian power grid hacking incident as the background, proposes to mine power big data and establish predictive models in the aspect of system interconnection; in the aspect of intelligent terminal protection, it proposes strict review and clear division of powers. Terminal intrusion warning; wireless security protection proposes the use of dedicated wireless channels and two-way encryption of communication data packets, and three aspects including targeted protection suggestions for the construction of the global energy Internet and grid security, and call on countries around the world to pay attention to the problems faced by the energy Internet Cyber risks and challenges. Literature [15] expands the model method based on the traditional power risk transmission model, uses binary composite network, interdependent complex network and simulation, and other methods to conduct research, and establishes a three-dimensional risk transmission model. The literature [16] summarized the three aspects of energy-agricultural coupling behavior modeling method, security risk mechanism analysis method, online security analysis method, etc., researched online security comprehensive analysis method based on data-knowledge fusion machine learning and provided early warning for energy Internet security Intelligence provides a theoretical basis. Current research is mainly focused on passive defense, unable to counter cyberattacks on time, and lacking methods and tools for online security situation prediction and analysis.

In recent years, neural networks have been widely used in speech, image, natural speech processing, and other fields. Literature [17] applied neural networks to prediction problems, and proposed a security situation prediction model based on RBF neural networks; literature [18] is an accurate grasp of the network security situation, a network security situation prediction method based on Elman neural network is proposed. Literature [19] focuses on the research status and application strategies of deep learning in natural language recognition and looks forward to the future development trend and difficulties of deep learning in natural language. Literature [20] applies deep learning to the transient stability assessment of power systems, which verifies that its method meets both accuracy and rapidity, and provides a new solution for transient stability analysis.

This paper studies the security risks faced by the regional energy Internet and uses the TCN-LSTM model to predict and analyze the security situation of the regional energy Internet. According to the various influencing factors of the Regional Energy Internet, obtaining a network security situation data set, preprocessing the security situation data, using Pearson Correlation to select features, retaining important features, and then dividing the data set into the training set and test set. The training set is used to train the TCN-LSTM model, and the test set is used to evaluate the pros and cons of the model.
2. Conceptual Basics

2.1. Temporal Convolutional Network (TCN, Temporal Convolutional Network)
Convolutional Neural Networks (CNN, Convolutional Neural Network) extracts important information from local input tiles through convolution calculations and retain the two-dimensional characteristics of the tiles, which makes it perform well in the field of computer vision. CNN uses a convolution kernel with a size of \( k \times k \) to extract features of the tiles, reducing parameters while retaining the spatial information of the tiles. Its variant Temporal Convolutional Neural Network (TCN) is widely used to process sequence models. By setting a convolution kernel with a size of \( k \times 1 \), convolution operations are performed in the time dimension to expand a one-dimensional data set to a multi-dimensional data set. To make it more in line with LSTM prediction\(^{[21]}\). Compared with RNN, the cost is much smaller in both time and space. Therefore, the temporal convolutional neural network can be effectively used to extract the key information of the local time series from the time series. In this way, we can preprocess the data.

2.2. Long short-term memory (LSTM, long short-term memory)
Long short-term memory (LSTM) is a variant of the recurrent neural network (RNN). It adds a method of carrying information across multiple time steps, that is, data information can be stored at any position in the time dimension. Input to the model, transfer to a later time step and pass it back intact when needed. This is the LSTM model idea. It saves information for future use and prevents early signals from disappearing and losing information during processing.

There are four important elements in the LSTM model: unit state, input gate, forget gate, and output gate. Input, forget and output gates are used to control the update, maintenance, and deletion of information contained in the unit state\(^{[21]}\). The extra data stream in Figure 2 carries information that spans time steps. Its value in different time steps is called \( C' \), where \( C \) stands for carrying.

![Figure 1 Model flow chart](image)
Figure 2 The internal principle of LSTM

\[ z = \tanh \left( W'x' : h'^{-1} \right) \]  
\[ z^i = \sigma \left( W'^i x' : h'^{-1} \right) \]  
\[ z^f = \sigma \left( W'^f x' : h'^{-1} \right) \]  
\[ z^o = \sigma \left( W'^o x' : h'^{-1} \right) \]  
\[ c^t = z^i \odot c'^{-1} + z^f \odot z \]  
\[ h^t = z^o \odot \tanh (c^t) \]  
\[ y^t = \sigma \left( W'h^t \right) \]  

\( x' \) is the data input in the current state, \( h'^{+1} \) is the input of the previous node, \( h^t \) is the output passed to the next node, \( c'^{-1} \) is the information carried by the previous node, and \( c^t \) is the information carried by the next node. \( y^t \) is the output in the current state, and \( W, W'^i, W'^f, \) and \( W'^o \) are the corresponding input, information, forget, and output weight matrices in the LSTM, respectively.

LSTM splices the current input \( x' \) and the \( h'^{-1} \) passed from the previous state, and then multiplies it with the corresponding weight matrix and trains it to obtain four states \( z, z^i, z^f, \) and \( z^o \). Among them, \( z^i, z^f, z^o \) are multiplied by the splicing vector by the weight matrix, and then converted into a value between 0 and 1 through a sigmoid activation function, and then as a gated state. And \( z \) is the result through an \( \tanh \) activation function is converted to a value between -1 and 1 (\( \tanh \) is used here because it is used as input data, not a gate signal)[27].

3. Modelling and its Analysis

3.1. Energy Internet security situation detection architecture
There are many smart devices in the energy Internet, such as smart power stations at the source end, community distribution networks at the network end, energy vehicles at the load end, smart charging piles at the energy storage end, etc. These devices upload data and share communication infrastructure. The generated data of these devices is analyzed by the Energy Internet, and the data analysis results are output to various devices to complete the regulation and management of the entire network. Every time data flows through a smart device, it will be attacked by hackers or malicious code, threatening the security of the Energy Internet. Direct attack refers to directly destroying equipment or the energy Internet; secondary attack refers to the attacker logging into the intelligent system in the energy Internet with a legal identity and controlling related servers by digging system vulnerabilities, raising permissions, etc., to obtain system permissions. Infiltrate attack the Energy Internet. Therefore, timely and accurate prediction of the security situation of the Energy Internet and ensuring the safety of its operation status is an urgent problem to be solved.

This article focuses on the regional energy Internet and divides common network attacks into four categories: PROBE port monitoring or scanning, DOS denial of service attacks, U2R unauthorized local superuser privileged access, R2L unauthorized access from remote hosts, these attacks will pose a gradual threat to the security situation of the Energy Internet, which is mainly reflected in the tampering of source data, such as power generation, power transmission path, and transmission; monitoring network data, such as energy router power receiving volume, power output path, output volume; destroying energy storage end data, such as power receiving volume, receiving source, power output volume, output path; embezzling load end data, such as load power consumption, load power source, Electricity price information, etc.

Figure 3 Architecture diagram of regional energy internet intrusion detection system

Set up security situation data collectors at each node of the Energy Internet to collect system operating status data, such as line load rate, load change rate, active power reserve rate, report number of report modules (reportnum), control module timeActivatedOperate (TAO) service Operating time (opertim), GSE module event sequence counter value (sqNUM), network communication protocol type (protocol type), number of access to system sensitive files and directories (hot), number of root user access (num_root), number of data packets(num_packets_router), etc. These Indexes are used as data characteristics, and then the security status of the system is scored using the analytic hierarchy process (AHP) based on the collected data set, and the security status of the system is obtained.
Table 1 The weight of each evaluation index

| Feature name                | Weights |
|----------------------------|---------|
| Line load rate             | 0.0928  |
| Load change rate           | 0.0739  |
| Active power reserve rate  | 0.1136  |
| Number of reports          | 0.1663  |
| TAO operation time         | 0.0836  |
| GSE count value            | 0.0638  |
| protocol type              | 0.0563  |
| hot                        | 0.1132  |
| num_root                   | 0.1039  |
| num_packets_router         | 0.1326  |

Concerning Protection Level 2.0, the security situation of the Energy Internet is divided into five levels, with white \((0 \leq F < 0.50)\), blue \((0.50 \leq F < 1.00)\), yellow \((1.00 \leq F < 1.50)\), orange \((1.50 \leq F < 2.00)\), and red \((2.00 \leq F < 2.50)\) indicating safety, general, early warning, heavier, and dangerous. Among them, the first and second levels of protection are general systems, and the supervision and management intensity are independent protection level and guidance protection level respectively; the third level of protection is important systems/critical information infrastructure, and the supervision and management intensity is the supervision protection level. And the fourth and fifth levels of protection are critical information infrastructure, and the intensity of supervision and management is respectively mandatory protection level and dedicated control protection level. The following figure shows the energy Internet security situation in the first quarter. The vertical axis represents the security situation value, and the horizontal axis represents the time. It is recorded every ten minutes and 144 times a day. It can be seen that the Energy Internet in the first quarter suffered four serious attacks, namely around the 17th of January, around the 2nd and 22nd of February, and at the end of March.

![Figure 4 Security situation map](image)

3.2. TCN-LSTM Hybrid Network Attack Detection Model
Long short-term memory (Long short-term memory, LSTM) is a special RNN that mainly solves the problems of gradient disappearance and gradient explosion during long sequence training. The model first uses the characteristics of TCN to be efficient, lightweight, and invariant to translation and preprocesses the time series security state data set through convolution and pooling. In the preprocessing stage, TCN extracts important information from the input data, transforms the one-dimensional input data into multi-dimensional feature data through the convolution kernel\[^{25}\], and converts the long input sequence into a short sequence composed of high-level features. Then, the short sequence is input into the LSTM again. LSTM controls the transmission state through the gating state, remembers the key indicators that require long-term memory, and forgets the insignificant indicators. This allows the model
to process longer sequences, view earlier data, and more accurately predict the next moment of the security status of the Energy Internet. Then this prediction result is transferred to the security attack comprehensive evaluation processing cloud for online detection and analysis, and finally, the monitoring and management of the security status of the Energy Internet is realized.

Figure 5 CNN-LSTM network architecture diagram

3.3. Experimental design
The device used in this article is the Windows10 64-bit operating system, processor bit Intel(R) Core(TM)i7-6700HQ CPU @2.60GHz, 8G memory, 1T hard drive, NVIDIA GTX960M 2G GDDR5 discrete graphics card. The TensorFlow framework and Keras deep learning tools are used for research and development.

Figure 6 Curve of energy internet security situation in the past ten days
Combining the energy Internet security situation map and common sense, it can be seen that the attackers are more active during the day, and the system security situation shows periodic changes. The
data of seven days a week is selected as the sample, and the data of the next day is used as the predicted value, and the "7+1" Method of rolling forecast of the security situation is adopted. Data is collected every ten minutes, six times per hour, and a total of 144 data are collected every day. The security situation data set is then divided into a training set, validation set, and test set. Before the test, the data is standardized, and then the Pearson correlation coefficient of each feature is calculated separately, the features with larger correlation coefficients are retained, and the smaller features are eliminated, to reduce the dimensionality of the sample space, reduce the complexity of the model and improve the operating efficiency while ensuring the quality of the model. Then use TCN temporal convolutional neural network to extract features on the data, convert the long input sequence into a short sequence composed of key features, and then use the extracted short sequence as the input of the LSTM neural network to train and predict the model.

3.4. Analysis and forecast

In this paper, two error evaluation indicators, mean absolute error and mean squared error, are used to evaluate the prediction results. The calculation formula is as follows:

\[
e_{MAE} = \frac{\sum_{i=1}^{n} |actual_i - predicted_i|}{n} \quad (8)
\]

\[
e_{MSE} = \frac{\sum_{i=1}^{n} (actual_i - predicted_i)^2}{n} \quad (9)
\]

Where: \( n \) is the total number of predicted samples; \( actual_i \) is the true value; \( predicted_i \) is the predicted value.

![Figure 7 CNN_LSTM training loss and verification loss](image)

It can be seen from the figure that the training loss continues to decrease, and the verification loss reaches the lowest at 25 epochs, the \( e_{MAE} \) value is 0.352, the \( e_{MSE} \) value is 0.2714, the model evaluation score is stable, and no overfitting is achieved.
Comparing the real data from Monday to Friday with the predicted data, it can be found that the security risks are mainly concentrated in the daytime, and it is safer at night, which is of guiding significance for the security defense of the Energy Internet. It can be seen from the figure that the predicted value of the model in the first two days is closer to the true value. When the system reaches a dangerous state, it can accurately predict and issue an alarm, and then gradually deviate from the true value. This also reflects the difficulty of predicting the sequence model and hard to predict the longer-term security status, but it has guiding significance for the protection measures and macro-control of the energy Internet. Because it is only necessary to predict the security status of the next day, it is not necessary and difficult to predict the security status of the next week.

When the energy Internet security situation is at the white level, the training, management, and confidentiality education of the staff should be strengthened, their security awareness should be improved, and a complete information security system should be formulated; when the security situation is at the blue level, monitoring and management should be strengthened such as the terminal equipment, Energy-information routers, relay protection devices, and power monitoring devices and other intelligent equipment; when the security situation is at a yellow level, the management and testing of the office system/network monitoring system of each unit should be strengthened, and U disk or mobile hard disk should not be used in Cross-use between equipment and networks; when the security situation is at the orange level, the office system/network of each unit should be isolated. It is strictly forbidden to open office documents or e-mails inside the system, and immediately check the security status of each unit, communication equipment, etc., and remove risk as soon as possible; When the security situation is at the red level, all systems and networks should be immediately isolated, non-essential servers, energy-information routers, critical information infrastructure, and other equipment should be shut down, and all units should be coordinated to adopt a unified security strategy. All forces and means are mobilized to deal with security risks, and professional security personnel should immediately intervene in the investigation.

4. Conclusion
This paper proposes a TCN-LSTM based energy Internet security situation prediction and assessment model, uses the AHP to obtain the weight of each indicator, and then gives the current energy Internet security status to obtain the system's security situation. Firstly, it uses the Pearson correlation coefficient to select feature variables, then uses TCN to extract the features, and finally, uses LSTM to predict the security situation of the Energy Internet for the next day. The results demonstrate that the model has good stability and better guiding significance for the security protection of the energy Internet, and its practical application prospects are of great importance.

Acknowledgments
We would like to express our sincere gratitude to everyone who helped in this research work. This project is supported by National key Research and Development Plan Project Funding (2020 YFE0200600) and...
References

[1] LI, J.H. (2020) Overview of Cyber Security Threats and Defense Technologies for Energy Critical Infrastructure. J. Journal of Electronics & Information Technology., 42: 2065-2081.

[2] Srikantha, P., Kundur, D. (2015) Denial of service attacks and mitigation for stability in cyber-enabled powergrid. C. IEEE Power & Energy Society Innovative Smart Grid Technologies Conference. In: Washington. USA. pp. 1–5.

[3] Zhang, Z.G., Gong, S.P., Dimitrovski, A.D. (2013) Time synchronization attack in smart grid: Impact and analysis. J. IEEE Transactions on Smart Grid., 4: 87–98.

[4] Liu, Y., Ning, P., Reiter, M.K. (2011) False data injection attacks against state estimation in electric powergrids. J. ACM Transactions on Information and System Security., 14: 13.

[5] Yan, J., He, H.B., Zhong, X.G., et al. (2017) Q-learning based vulnerability analysis of smart grid against sequential topology attacks. J. IEEE Transactions on Information Forensics and Security., 12: 200–210.

[6] Xiang, Y.M., Ding, Z.L., Zhang, Y.C., et al. (2017) Power system reliability evaluation considering load redistribution attacks. J. IEEE Transactions on Smart Grid., 8: 889–901.

[7] Liu, S., Kundur, D., Zournotos, T., et al. (2012) Coordinated variable structure switching attack in the presence of model error and state estimation. In: The 3rd IEEE International Conference on Smart Grid Communications. Tainan, China. pp. 318–323.

[8] Sankar, L., Rajagopalan, S.R., Mohajer, S., et al. (2013) Smart meter privacy: A theoretical framework. J. IEEE Transactions on Smart Grid., 4: 837–846.

[9] Xu, R.Z., Wang, R., Guan, Z.T., et al. (2017) Achieving efficient detection against false data injection attacks in smart grid. J. IEEE Access., 5: 13787–13798.

[10] Ye, H.X., Ge, Y.Y., Liu, X., et al. (2016) Transmission line rating attack in two-settlement electricity markets. J. IEEE Transactions on Smart Grid., 7: 1346–1355.

[11] Ten, C.W., Hong, J., Liu, C.C. (2011) Anomaly detection for cybersecurity of the substations. J. IEEE Transactions on Smart Grid., 2: 865–873.

[12] Langner, R. (2011) Stuxnet: dissecting a cyberwarfare weapon. J. IEEE Security and Privacy Magazine., 9: 49-51.

[13] Ye, X.M., Wen, F.S., Shang, J.C., et al. (2015) Propagation Mechanism of Cyber Physical Security Risks in Power Systems. J. Power System Technology., 39: 3072-3079.

[14] Zhang, S.J., He, B., Wang, L.F., et al. (2016) The Enlightenment of Ukraine's Power Outage to the Security of Global Energy Internet. J. Electric Power Information and Communication Technology., 14: 77-83.

[15] Li, C.B., Li, X.P., Tian, S.M., et al. (2017) Energy Internet Power Information Deep Integration Risk Transmission: Challenges and Prospects. J. Automation of Electric Power Systems., 41: 17-25.

[16] Fu, X.Q., Zhou, Y.Z., Sun, H.B. (2020) Online Security Analysis of a Park-level Agricultural Energy Internet: Review and Prospect. J. Proceedings of the CSEE., 40: 5404-5411.

[17] Ren, W., Jiang, X.H., Sun, X.F. (2006) RBFNN-based Prediction of Networks Security Situation. J. Computer Engineering and Applications., 31: 136-138, 144.

[18] You, M.Y., Ling, J., Hao, Y.J. (2012) Prediction Method for Network Security Situation Based on Elman Neural Network. J. Computer Science., 39: 61-63, 76.

[19] Xi, X.F., Zhou, G.D. (2016) A Survey on Deep Learning for Natural Language Processing. J. Acta Automatica Sinica., 42: 1445-1465.

[20] Hu, W., Zheng, L., Min, Y., et al. (2017) Research on Power System Transient Stability Assessment Based on Deep Learning of Big Data Technique. J. Power System Technology., 41: 3140-3146.

[21] Liang, M., Mo, Y.C., Lin, D., et al. (2020) Disease Prediction model based on hybrid deep learning algorithm. J. Artificial Intelligence and Robotics Research., 9: 16-23.
[22] Li, Z.W., Tong, W.M., Jin, X.J. (2016) Construction of Cyber Security Defense Hierarchy and Cyber Security Testing System of Smart Grid: Thinking and Enlightenment for Network Attack Events to National Power Grid of Ukraine and Israel. J. Automation of Electric Power Systems., 40: 147-151.

[23] Yu, Q., Li, H., Qu, Y.Q. (2020) Research on security situation awareness of large power grid based on deep neural network and internal and external factors. J. Electrical Measurement & Instrumentation., http://kns.cnki.net/kcms/detail/23.1202.TH.20200417.1650.002.html.

[24] Lin, J.H., Fan, S.X., Xu, Z.Q. (2020) A Situation Awareness Model for Power Grid Operation Based on Fuzzy Analytic Hierarchy Process and LSTM-Attention Mechanism. J. Electric Power Information and Communication Technol., 18: 58-66.

[25] Su, X.Y., Xu, K.K. (2020) Research status of multi-source heterogeneous data fusion algorithm in network security situation awareness. J. Journal of the Hebei Academy of Sciences., 37: 37-44.

[26] Yan, J.H., Hou, M.M. (2020) Study on Time Series Prediction of Theft Crime Based on LSTM Network. J. Data Analysis and Knowledge Discovery., https://kns.cnki.net/kcms/detail/10.1478.G2.20200910.1451.002.html.

[27] Gong, G.J., Mahato, N.K., He, H., et al. (2020) Transient Stability Assessment of Electric Power System based on Voltage Phasor and CNN-LSTM. In: 2020 IEEE/IAS Industrial and Commercial Power System Asia (I&CPS Asia). Weihai, China. pp. 443-448.