Data transmission of cyber physical power system

Yishuang Hu1,3, Zhengwei Jiang2, Yikai Sun7, Yi Ding1, Chenbo Xu2 and Xueqi Jin2

1 College of Electrical Engineering, Zhejiang University, 310027, Zhejiang province, China;
2 State Grid Zhejiang Economic Research Institute, Hangzhou, 310007, Zhejiang province, China
3 Email: 273415335@qq.com

Abstract. Aiming at monitoring the behaviour of power system to make it work correctly and better, cyber physical power system (CPPS) was introduced. However, due to the high integration of cyber system, the complexity of power system is greatly enhanced, which puts forward higher requirements for the reliable and safe operation of CPPS. Moreover, when the cyber system is under attack, abnormal information flow may lead to abnormal energy flow. Therefore, this paper proposes a data transmission mechanism to analyse the information flow among CPPS. A data transmission optimization model based on the transmission matrix is constructed. The data transmission from the cyber system to the power system is quantified by the model. The practicability of the proposed data transmission mechanism is given by numerous cases.

1. Introduction

Recently, driven by the worldwide wave of energy conservation and the rapid development of information technology, the power system is undergoing profound changes [1]. The integration of power system with energy systems and cyber systems is accelerating with an unprecedented speed [2]. Totally speaking, the traditional power system is undergoing a fundamental change, the power system is transformed into a more widely, intelligently, flexibly and safely system [3].

In order to speed up such transformation, the integration of advanced information and communication technologies are particularly critical for power system. Then cyber physical power system (CPPS) was introduced [4]. CPPS aims at monitoring the behavior of physical processes, and actuating actions to change its behavior in order to make the physical environment work correctly and better. Typically, the physical process is monitored or controlled by the cyber system, which is a networked system of several tiny devices with sensing, computing and communication capabilities [5]. At present, there are many researches on CPPS, such as modeling, controlling, scheduling, and security defense. Reference [6] proposed a method for quantitative evaluation of the risk transmission threshold of power CPS networks based on the percolation theory. A robust Cubature Filter based approach was proposed for dynamic state estimation of CPS [7].

However, due to the high integration of cyber system and power system, the complexity of operation and control of CPPS is greatly enhanced, which puts forward higher requirements for the reliable and safe operation of CPPS. Therefore, it is urgent to carry out the research of CPPS modeling techniques for engineering practical usage. Meanwhile, with the cyber system playing an increasingly important role in CPPS, it may cause serious consequences if the cyber system is under attack. When
the cyber system is under attack, abnormal information flow may lead to abnormal energy flow, which in turn endangers the safety and stability of the power system. Therefore, the security of data transmission of cyber system is also a prerequisite to ensure the safe operation of CPPS and to avoid the occurrence of power outage. The consequence of cyber system data transmission must be reflected by the modeling technique of CPPS.

Concerning the strong relationship between cyber system and power system, this paper proposes a data transmission mechanism to analyze the information flow among CPPS. Data transmission is divided into data transmission in cyber system, in power system, and between power and cyber systems. There are nodes and communication channels among them. A data transmission model based on the transmission matrix is established. The data transmission from the cyber system receiving end to the power system sending end is quantified by the model.

The remainder of this paper is organized as follows. Section 2 presents the framework of data transmission. Section 3 constructs the data transmission mechanism under the information flow of cyber system. Case studies are carried out in Section 4 to illustrate the proposed mechanism. Finally, conclusions are drawn in Section 5.

2. Framework of data transmission of CPPS

CPPS is a combination of power system and cyber system, which includes the characteristics of power flow in power system and information flow in cyber system. Compared with traditional power systems, CPPS pays more attention to the impact of massive information flow on power system. Compared with traditional cyber systems, CPPS focuses more on how to convert information flow of cyber systems into power data that can be processed by power system, so as to realize the interaction between power flow and information flow. The data transmission in CPPS is reflected in Figure 1.

The meaning of data transmission used in the paper is the process of data transmitted from the receiving end of cyber system to the sending end of power system. There are complicated connections among CPPS. In CPPS, the data of the cyber system is transmitted to the power system, which leads to a continuously transmitted to the adjacent, sub-adjacent elements and further elements [8], [9].

The data transmission of CPPS can be divided into three parts: the first part is the data transmission from the receiving end to the sending end of cyber system. The second part is the data transmission from the sending end of cyber system to the receiving end of the power space. The third part is the data transmission from the receiving end to the sending end of power system. There are nodes and communication channels in CPPS. Nodes refer to devices in cyber and power systems. Communication channels represent the channels for data transmission among CPPS. The sending end of the cyber system refers to the corresponding devices that can send data in the cyber system, such as wireless signal transmitter, optical fiber laser transmitter, oscilloscope, etc. The receiving end of power system refers to the corresponding devices that can accept data in the power system, such as voltage sensor, current sensor, frequency detector and so on.

However, due to the high integration of cyber system and power system, the complexity of operation and control of CPPS is greatly enhanced, which puts forward higher requirements for the
reliable and safe operation of CPPS. Therefore, it is urgent to carry out the research of cyber system data transmission. Data from the sending end of the cyber system, passing through a myriad of components, until the receiving end of power system can obtain the data. Because the components in the transmission do not guarantee perfect data transmission, the data from the sending end of cyber system cannot be absolutely predicted when transmitted to the receiving end of power system. However, it is possible to infer the final transmission result of a particular data according to the transmission situation of historical data. The data transmission mechanism studied in this paper is expected to reflect the data transmission from the sending end of the cyber system to the receiving end of the power system. The data transmission mechanism studied in this paper is emphasized on the data transmission process among CPPS, which can give a result prediction about an unknown data from cyber system. Unlike the researches in [10] [11], these paper mainly focus on how to make a better use of the data when it arrives in the power system. This paper is about the data result before the power system.

3. Data transmission mechanism of CPPS

3.1. Data transmission matrix

Data transmissions inside the cyber system and power system have been comprehensively studied [12], [13]. The unique characteristics of CPPS are the interaction between cyber system and power system. Therefore, this paper concentrates on the data transmission between cyber system and power system. The data transmission matrix focuses on the nodes from the sending end of cyber system and from the receiving end of power system, along with the communication channels among these two systems [14].

Assume the whole CPPS contains \( n_1 \) nodes from the sending end of cyber system and \( n_2 \) nodes from the receiving end of power system. The contained data under a certain period of time is referred as the data state of this node. Therefore, the data state vector of the sending end of cyber system is written as \( D = [d_1, d_2, ..., d_{n_1}] \). \( d_i \) is the data state of node \( i \) in the sending end of cyber system. The data state vector of the receiving end of power system is written as \( D' = [d'_1, d'_2, ..., d'_{n_2}] \). \( d'_i \) is the data state of node \( i \) in the receiving end of power system.

\[
\bar{D}' = [D, D'] = [d_1, d_2, ..., d_{n_1}, d'_1, d'_2, ..., d'_{n_2}]
\]

is the data state vector of CPPS containing all the necessary nodes. There are communication channels between cyber system and power system. But these channels are not perfectly working and the data may be damaged when transmitting through these channels. Thus, a transmission probability \( p_{i,j} \) is defined in this paper, which describe the data transmission success rate between node \( i \) and node \( j \). Nodes \( i \) and \( j \) can be both in cyber system or power system. As the data of cyber power can be transmitted into other nodes in the cyber system, as well. For instance, node 1 contains \( d_i \) data that need to be transmitted to node 2, while the transmission probability for the communication channels is \( p_{1,2} \), then the receiving data of data 2 is \( d_2 = d_1 \cdot p_{1,2} \). The data transmission matrix consists of multiple transmission probabilities \( p_{i,j} \) between nodes from cyber system and power system, which can be denoted as:

\[
P = (p_{i,j})_{(n_1+n_2)\times(n_1+n_2)} = \begin{bmatrix}
p_{i,1} & p_{i,2} & \cdots & p_{i,(n_1+n_2)} 
p_{j,1} & p_{j,2} & \cdots & p_{j,(n_1+n_2)} 
\vdots & \vdots & \ddots & \vdots 
p_{(n_1+n_2),i} & p_{(n_1+n_2),2} & \cdots & p_{(n_1+n_2),(n_1+n_2)}
\end{bmatrix}
\]  

(1)

where \( p_{i,j} \) is the data transmission success rate between node \( i \) and node \( j \). Nodes \( i \) and \( j \) are the nodes from the sending end of cyber system and the receiving end of power system.
3.2. Data transmission matrix calculation model

It can be noted from the data transmission matrix that transmission possibilities are the core of this matrix. The calculation of data transmission matrix is the calculation of transmission possibilities.

There are lots of datasets containing the data state of each node during the historical data transmission. Thus, this paper applies an optimization model to make a better usage of these datasets.

Suppose \( D_t = \left[ d_1^t, d_2^t, \ldots, d_n^t \right] \) is the historical data state vector of CPPS in time period \( t \), which contains all the data state of nodes from the sending end of cyber system and the receiving end of power system. It requires a unit of time for the data transmitting from cyber system to power system.

\[ D_{t+1} = \left[ d_1^{t+1}, d_2^{t+1}, \ldots, d_n^{t+1} \right] \]

\( D_{t+1} \) is the calculated data state vector of CPPS in time period \( t+1 \), which can be evaluated by (2).

\[
\begin{align*}
\hat{D}_{t+1} & = (\bar{D} \cdot P) \cdot d_1^t, d_2^t, \ldots, d_n^t \end{align*}
\]

In order to obtain the data transmission matrix, an optimization model is proposed to minimize the sum of error squares between the historical data state vector of CPPS and the calculated data state vector during the transmission periods.

This optimization model is established with the following formulas, through which the transmission probability of data transmission between each node can be obtained.

\[
\begin{align*}
\min & \ f(P) = \sum_{t=0}^{m-1} \left( \hat{D}^{t+1} - (\bar{D} \cdot P) \right) \left( \hat{D}^{t+1} - (\bar{D} \cdot P) \right) \\
\text{s.t.} & \quad P_{i,j} \geq 0
\end{align*}
\]

where \( \bar{D} \) is the data state vector of CPPS in time period \( t \), \( \hat{D}^{t+1} \) is the data state vector of CPPS in time period \( t+1 \), \( f(P) \) is the sum of error squares. This data transmission contains \( m \) time periods, which means the data state of each node is stable after \( m \) time periods.

3.3. Data transmission mechanism

By applying different historical data transmission process, the value of \( \bar{D} \) and \( \hat{D}^{t+1} \) can be achieved. The matrix \( P \) is the calculated value in this optimization model. Suppose random values of elements in \( P \) and submitted into the model. Minimizing the sum of error squares between the historical data state vector of CPPS and the calculated data state vector during the transmission periods, the values of elements in \( P \) are constantly modified by different historical data transmission process. And finally the best matrix \( P \) can be evaluated.

This paper pays more attention to the prediction of data transmission results. From the perspective of historical data transmission results, it finds the variation of data transmission probability between various nodes in various data transmission processes. Therefore, the data transmission probability of each node can only be unified from the perspective of probability to obtain a probability value that can represent the characteristics of the node. This paper adopts the historical data transmission process to calculate. Considering the large numbers of the transmission of historical data, every data transmission leads to different node data transmission probability, so it is necessary to adopt an optimization model, where all of the data transmission process are unified to consider. By minimizing the sum of error squares, the error of each data transmission process is minimized, that is, transmission process is unified.
The data transmission matrix is evaluated by the historical transmission process and the optimization model mentioned above. Thus, the completely data transmission with a known initial data state vector of cyber system can be formulated.

Suppose \( D^0 \) is the initial data state vector of CPPS in time period 0, while during the other time periods \( D^{t+1} \) is unknown. Based on the calculated data transmission matrix \( P \), the calculated data state vector \( \tilde{D}^{t+k} = [\tilde{d}_1^{t+k}, \tilde{d}_2^{t+k}, ..., \tilde{d}_{n+\,\,t+k}^{t+k}] \) during the other time periods can be assessed by (4) and (5).

\[
\tilde{d}_j^{t+k} = \sum_{i=1}^{n+\,\,t+k} \tilde{d}_i^t \cdot P_{i,j} \quad (4)
\]

\[
\tilde{D}^t = \tilde{D}^0 \cdot P, \quad \tilde{D}^{t+k} = \tilde{D}^0 \cdot P \cdot P = \tilde{D}^0 \cdot P^{k+1} 
\]

The data transmission is finished until \( \tilde{D}^{t+k} \) is stable, then the final data state \( \tilde{d}_j^{t+k} \) of node \( j \) is the contained data of node \( j \) eventually.

4. Case study

In this section, we analyze a data transmission of a CPPS [15]. The construction of CPPS can be seen in Figure 2.

![Figure 2. CPPS.](image)

There are three nodes in the cyber system, denoted as \( r_1, r_2, r_3 \). There are three nodes in the power system, noted as \( r_1', r_2', r_3' \). Based on the historical data transmission, the data transmission matrix can be calculated by the optimization model, which is

\[
P = \begin{bmatrix}
0.21 & 0.22 & 0.16 & 0.21 & 0.03 & 0.16 \\
0.18 & 0.13 & 0.10 & 0.20 & 0.18 & 0.22 \\
0.20 & 0.21 & 0.15 & 0.04 & 0.04 & 0.36 \\
0.19 & 0.08 & 0.32 & 0.09 & 0.21 & 0.11 \\
0.10 & 0.21 & 0.02 & 0.15 & 0.22 & 0.03 \\
0.13 & 0.17 & 0.24 & 0.19 & 0.21 & 0.05
\end{bmatrix}
\]

Case 1: Based on the data transmission matrix, the data transmission mechanism of this CPPS can be evaluated. Assume the initial data vector of the sending end of cyber system is \( D^0 = [1, 0.2, 0.5] \) and initial data vector of the receiving end of power system is \( D^0 = [0, 0, 0] \). The data transmission of each node can be seen in Figure 3.
Case 2: Assume the initial data vector of the sending end of cyber system is \( D^0 = [1, 0.2, 0.5] \) and initial data vector of the receiving end of power system is \( D^0' = [0, 0, 0] \). After the third time period, there are an added data 1 on node \( r_2 \). The data transmission of each node can be seen in Figure 4.

![Figure 3. Data transmission of CPPS in case 1.](image)

![Figure 4. Data transmission of CPPS in case 2.](image)

Case 3: Assume the initial data vector of the sending end of cyber system is \( D^0 = [1, 1, 0.2] \) and initial data vector of the receiving end of power system is \( D^0' = [0, 0, 0] \). After the third time period, there are an added data 1 on node \( r_2 \). The data transmission of each node can be seen in Figure 5.

![Figure 5. Data transmission of CPPS in case 3.](image)

It can be seen from Figure 3 that node \( r_3' \) is the most influenced node after this data transmission, while node \( r_1 \) is less influenced. In Figure 4, node \( r_1 \) is the most influenced node and node \( r_3 \) is less influenced as well. In Figure 5, node \( r_3' \) is the most influenced node and node \( r_2 \) is less influenced as well. Moreover, after the transmission of each node, the data of each node having is completely changed. This is also the reflection of information interaction of CPPS.

5. Conclusions
Combining with sensing, computing and communication devices, the CPPS has been widely used. However, due to the high integration of cyber system and power system, it is urgent to carry out the research of cyber system data transmission as the cyber system in CPPS is a significant part. However, because the components in the transmission do not guarantee perfect data transmission, the data from the sending end of cyber system cannot be absolutely predicted when transmitted to the receiving end of power system.

According to the characteristics of the CPPS, the paper establishes a data transmission mechanism expecting to reflect the data transmission from the sending end of the cyber system to the receiving end of the power system. The data transmission mechanism studied in this paper is emphasized on the data transmission process among CPPS, which can give a result prediction about an unknown data from cyber system. Constructed by the transmission matrix and the optimization model to solve the
data transmission matrix, the proposed data transmission matrix fully reflects the data transmission process between the cyber system and power system. Because the characteristics of each node will vary from source to source, it is impossible to absolutely predict. Therefore, the data transmission probability of each node can only be unified from the perspective of probability. By adopting the historical data transmission process, the impact of cyber system information flow on data transmission of CPPS can be analyzed. It can be found through cases that different nodes have been differently influenced. Moreover, after the transmission of each node, the data of each node having is completely changed. The presented case reveals the practicability and convenience of the data transmission mechanism of CPPS.

With the help of data transmission mechanism in this paper, the future work can be monitor and protection studying about CPPS.

Acknowledgement

The research is supported in part by the Science and Technology Project of State Grid Zhejiang Electric Power Co., Ltd under Grant 5211JY180012.

Reference

[1] Xiaoxin Z, Shuyong C, Zongxiang L 2018 Technology Features of the New Generation Power System in China Proceedings of the CSEE 38 1983-1904
[2] Yun W, Dong L, Jiaming W 2018 The Research of Power CPS Modeling and Simulation Verification Platform Proceeding of the CSEE 38 130-136
[3] Han Y, Wen Y, Guo C 2015 Incorporating Cyber Layer Failures in Composite Power System Reliability Evaluation Energies 8 9064-9086
[4] Sun X 2015 Cyber-physical Modeling and Cyber-contingency Assessment of Hierarchical Control Systems IEEE Tran. on Smart Grid 6 2375-2385
[5] Wang K, Ye Y, Xu X 2010 Security Issues and Challenges for Cyber Physical System IEEE/ACM Int. Conf. on Green Computing & Communications & Intl Conference on Cyber. IEEE Computer Society 2010
[6] Qu Z, Zhang Y, Qu N 2018 Method for Quantitative Estimation of the Risk Transmission Threshold in Electric Power CPS Based on Seepage Probability IEEE Access 99 1-10
[7] Yang Li, Zhi Li, Liang Chen 2019 Dynamic State Estimation of Generators under Cyber Attacks IEEE Access 99 1-10
[8] Kundur D, Feng X, Shan L Towards a Framework for Cyber Attack Impact Analysis of the Electric Smart Grid IEEE Int. Conf. on Smart Grid Communications 2010
[9] Hahn A, Govindarasu M 2011 Cyber Attack Exposure Evaluation Framework for the Smart Grid IEEE Tran. on Smart Grid 2 835-843
[10] Chen C, Yan J, Lu N 2015 Ubiquitous Monitoring for Industrial Cyber-Physical Systems Over Relay- Assisted Wireless Sensor Networks IEEE Tran. on Emerging Topics in Computing 3 352-362
[11] Yu J, Shen Y, Okyay K 2018 Data-Driven Monitoring and Safety Control of Industrial Cyber-Physical Systems: Basics and Beyond IEEE Access 1 1-12
[12] Hua Y, Liu Y, Peng Z 2016 Efficient Eigen-Analysis for Large Delayed Cyber-Physical Power System Using Explicit Infinitesimal Generator Discretization IEEE Tran. on Power System 31 2361-2370
[13] Wu G, Sun J, Chen J 2018 Optimal Data Injection Attacks in Cyber-Physical Systems IEEE Tran. on Cybernetics 99 1-11
[14] Zhen H, Cheng W, Stojmenovic M 2015 Characterization of Cascading Failures in Interdependent Cyber-Physical Systems IEEE Tran. on Computers 64 2158-2168
[15] Ye H, Mou Q, Liu K 2018 Modeling and Formulation of Delayed Cyber-Physical Power System for Small Signal Stability Analysis and Control IEEE Tran. on Power Systems 25 1-11