The Design and Implementation of Attack Path Extraction Model in Power Cyber Physical System

Lei Wang, Zhaoyang Qu, and Zelong Li
School of Information Engineering, Northeast Dianli University, Jilin 132012, China
Email: neduwanglei@qq.com; qzywww@mail.nedu.edu.cn; 531146846@qq.com;

Abstract —In the attack of power Cyber Physical System (CPS), the key problem of taking effective response to the defense measures is how to extract the attack path quickly and accurately. This paper proposes an attack path extraction model based on Hidden Markov Model (HMM). Firstly, the original state sequence of information communication system and electric system must be processed by the representing, filtering, segmenting and fusion, then receiving the joint sequence of system failure that produced by the same attacker; Secondly, on the basis of the designed mapping table between information physics cooperative attack and system failure, system failure probability matrix can be generated dynamically. Meanwhile, the concept of sensitivity matrix is introduced to quantitative analyze the interaction effects between information attacks and physical attacks. Finally, the implementation algorithm of the model is given. The experimental results show that the proposed model can effectively extract the most likely sequence of attack path based on the known sequence of the system failure.

Index Terms—Power cyber physical system, attack path extraction, the joint sequence of system failure, hidden markov model

I. Introduction

Information communication system and the physical system closely fused in the modern power system that from the complex coupling network, many scholars regard this system as power CPS. This change makes the grid attack is no longer isolated or a single form, it has consist of coordinated attack sequence that has certain timing and complex relationship [1]. The typical attack process can be illustrated as follows: the malicious attackers intrude EMS or SCADA secondary information system through virus, script, brute force and other means of hacker, this process can be called for the original information attack [2]. After the invasion succeed, the attacker will achieve advanced operating permissions of related system, and then the attacker will sends a error decision order, that resulting in physical system abnormalities in the power grid, this process can be called secondary physical attack.

Such a new form attacks that oriented power CPS has the following characteristics: 1) it has a clear attack target; 2) the power grid operation will be damaged in different degrees; 3) the attacker intent to design a complex attack sequence. Only a clear grasp of the complete attack steps in order to establish an active information security defense strategy, therefore, the key problem of achieving security defense is how to extract the attack sequences [3].

Based on the above analysis, this paper designs the attack path extraction model based on Hidden Markov Model (HMM). The basic idea can be described as follows: To begin with, the original state sequence of information communication system and electric system must be processed by the representing, filtering, segmenting and fusion, then receiving the joint sequence of system failure that produced by the same attacker. What's more, on the basis of the designed mapping table between information physics cooperative attack and system failure, system failure probability matrix can be generated dynamically. Meanwhile, the concept of sensitivity matrix is introduced to quantitative analyze the interaction effects between information attacks and physical attacks. At last, the experimental results show that the model has better effect on the attack path dependence [4].

II. Power Cyber Physical System Attack Path Extraction Model Definition

According to HMM model, this paper defines the attack path extraction model, it can be represented by a five tuple $W=<N, M, \pi, \mathbf{B}, A>$.

Definition 1: information Physics cooperative attack sequence set $N=\{n_1, n_2, n_3, \cdots n_{\max N}\}$, $0<i\le \max N$.

Definition 2: system fault joint sequence set $M=\{m_1, m_2, m_3, \cdots m_{\max M}\}$, $0<j\le \max M$.

Definition 3: attack sequence initiation probability π, $\pi=\{\pi_i\}$.

Definition 4: system failure probability matrix $\mathbf{B}=\{b_{ij}\}$, $b_{ij}=P(o_t(j)\,|\,q_t(i))$, $\sum_{j=1}^{\max M} b_{ij}=1$, $0<j\le \max M$, where $o_t(j)$ is some kinds of system failure j occurs at time t, $q_t(i)$ is some kinds of attack methods i occurs at time t, b_{ij} is the probability of a class of system failure is caused by an attack at some point.

Manuscript received June 7, 2016; revised September 25, 2016.
This work was supported by the National Natural Science Foundation of China under Grant No.51277023, and the Science and Technology Development Plan of Jilin Province under Grant No.20140307008GX.
Corresponding author email: 752953593@qq.com.
doi:10.12720/jcm.11.9.834-840

Definition 5: information and physical interaction impact sensitivity matrix $\mathbf{A}=\{a_{ij}\}$, $a_{ij}=P(q_t(j)|q_{t-1}(i))$, $\sum_{j=1}^{\max N} a_{ij}=1, 0<i,j\le \max N$, where a_{ij} is the conditional probability of the attack n_j occurred in the case of the previous attack n_i.

III. The Construction of Attack Path Extraction Model in Power Cyber Physical System

Attacks may occur in the power generation, transmission, substation, distribution, electricity or any link against the power CPS. Although the attack scene is different, the overall form and process is basically the same [5]. Therefore, in the study, we select the Intrusion Detection System (IDS) in power network as the analysis object of information system operation state, in the transmission link we select the Energy Management System (EMS) as the analysis object of grid operation state [6]. The construction of the model is divided into three main stages:

1) Getting the joint sequence of system failure produced by the same attacker; 2) Designing mapping table between information physics cooperative attack and system failure, then constructing the probability matrix of system failure based on the above mapping table; 3) Determine the sensitivity matrix of the interaction effects between information attacks and physical attacks. The process of the model building is shown in Fig. 1.

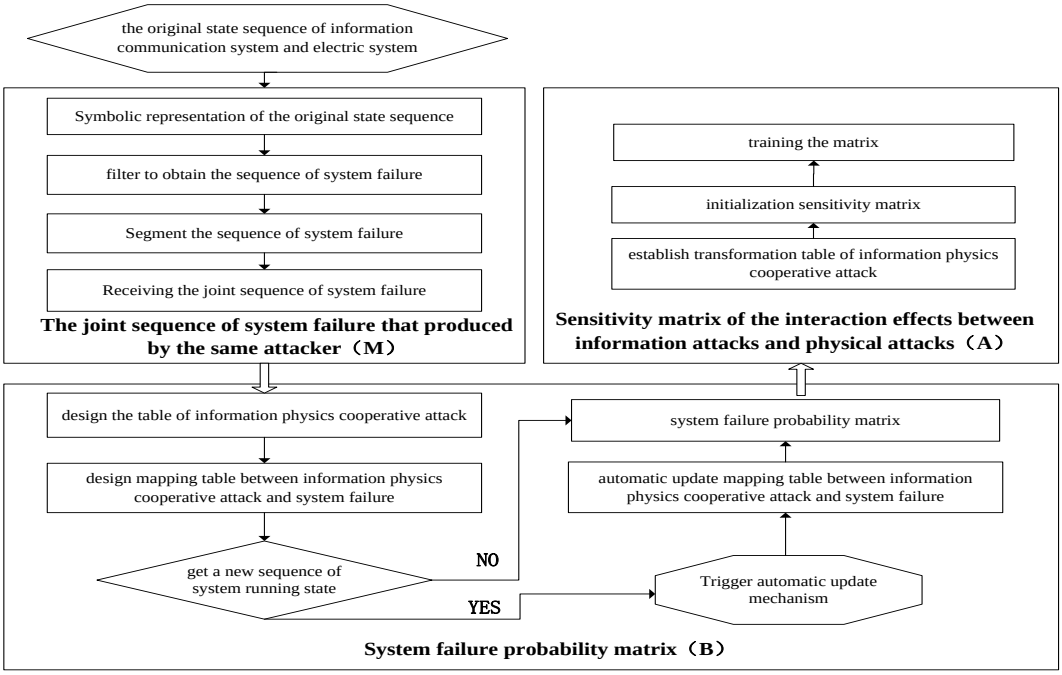

Fig. 1. The process of attack path extraction model building

A. Getting the Joint Sequence of System Failure Produced by the Same Attacker

In order to extraction the path of information physics cooperative attack, the first work need to get all system failure sequence produced by the same attacker [7]. Considering information attack sequence and fault sequence of power grid operation come from different systems: IDS and EMS, there are great differences existed in the content and performance of the two system. The following four steps are designed to obtain the joint sequence of the system failure sequence generated by the same attacker.

Step 1: Symbolic representation of the state monitoring sequence

The representation of monitoring sequence "IS" of the information system. Such monitoring sequence is real-time achieved through the deployment of IDS between the power intranet and extranet boundary. Each record contains the following information: T (time), IP (the IP address of attack source), Hostname, M (system failure), Event (the attack event), Sig_name (alert name) Sig _pri (alert priority), the sequence of attributes set is expressed as:

IS={T, IP，Hostname，M，Event，Sig_name，Sig_pri}

The representation of monitoring sequence "OS" of the state of power grid operation. Through the EMS system according to the telemetry, real-time statistics information, we can judge the running state of the transmission system. Each record contains the following information: T (time), StationName (the station name), Device (equipment device), M (system failure), Value (actual value or difference value), Exception_type (abnormal information type), the sequence of attributes set is expressed as:

OS={T, StationName，M，Device，Value, Exception_type}

Step 2: Filtering the state monitoring sequence to obtain the sequence of system failure

Fault information and the normal operation information are contained in the sequence of state monitoring sequence, we focus on the analysis of all kinds of sequence of system failure. The state sequence "IS" and "OS" are respectively processed based on the filtering rule that setting the threshold, all the normal operation information can be eliminated.

Step 3: segmenting the sequence of system failure

The sequence of information system failure is divided according to the IP address attribute, we can obtain independent subset IS_n of information system failure. Similarly, the sequence of physical system failure is divided according to the StationName attribute, we can obtain independent subset OS_m of power grid operation failure.

Step 4: getting the joint sequence of system failure

Information system failure sequence subset IS_n and power grid operation failure sequence subset OS_m are sorted respectively according to the Time attribute. By setting the time window threshold t_d, the starting and stopping time interval for the sequence IS_n is $[t_i, t_{i+n}]$, the time interval of the sequence OS_m is $[t_j, t_{j+m}]$, the conditions of the two subsets merging are as follows:

Condition 1: $\forall t_i < t_j < t_{i+n}$

Condition 2: $\forall \left| t_{j+m} - t_{i+n} \right| < t_d$

If the sequence can meet any of the above conditions, that is to say, the occurrence of the two sequences is related to a large degree, IS_n and OS_m will be merged. According to Time attribute the merged sequence can be new sorted, we will get a joint sequence of system failure generated by the same attacker K step attack. Expressed as $M = \{M_1, M_2, M_3, \cdots M_k\}$.

B. Determine Probability Matrix of the System Failure

(1) The mapping table between information physics cooperative attack method and system failure

According to the evaluation index of electric power enterprise information and communication process, also the security evaluation standard or specification in the electric secondary system, combing the experience of the experts in this area [8], we sort out a list of common attack methods for power CPS, a mapping table of information physics cooperative attack method and system failure, as shown in Table I, Table II.

TABLE I: LIST OF COMMON ATTACK METHODS

attack method number	attack type	attack method
I1	Information attack	DDOS
I2	Information attack	Black Hole Attack
I3	Information attack	Change communication network topology
I4	Information attack	Error Data injection
I5	Information attack	Man in the middle attack
I6	Information attack	Replay attack
I7	Information attack	Profiteering password cracking
I8	Information attack	Malware and viruses
I9	Information attack	Use of internal staff
E1	Physical attack	Malicious change switch status
E2	Physical attack	Error scheduling instruction
E3	Physical attack	The device parameters and the field is not consistent
E4	Physical attack	Increase weight setting deviation
E5	Physical attack	Error in connection between devices
E6	Physical attack	Make the equipment overload
E7	Physical attack	The closing loop break
E8	Physical attack	Causes the control circuit to appear the question
E9	Physical attack	Appeared through the short circuit

TABLE II: SYSTEM FAILURE–ATTACK METHODS MAPPING TABLE

fault number	fault name	attack method number	Prior probability of failure occurrence
F1	Switch failure of power network operation	E1/E2	0.33/0.25
F2	Bus failure of power grid	E3/E4/E7/E8/E9	0.54/0.47/0.72/0.37/0.13
F3	Transformer failure of power network operation	E5/E6/E9	0.27/0.64/0.63
F4	PQI does not match	E7/E8	0.28/0.63
F5	Suspicious current measurement	E1/E2/E3/E4	0.31/0.25/0.46/0.53
F6	Transformer active reactive power imbalance	E2/E5/E6/E9	0.25/0.36/0.36/0.24
F7	Line active reactive power imbalance	E1/E2/E5	0.32/0.25/0.33
F8	Remote control of information system	I3/I7/I8	0.26/0.06/0.5
F9	Information system permissions are modified	I4/I5/I7/I9	0.17/1/0.94/0.3
F10	The information system is not accessible	I1/I2/I6/I9	0.21/1/1/0.3
F11	Information systems are being monitored	I8/I9	0.5/0.3
F12	The information system of network equipment downtime	I1/I3/I4	0.79/0.74/0.83

(2) The calculation of the probability matrix of the system failure

The probability matrix of the system failure B can be computed through importing Table I and Table II. Among $\mathbf{B} = \{b_{ij}\}$, row vector represents the number of attack method, and column vector represents the system fault number.

(3) Designing automatic update method in the mapping table of cooperative attack method and system failure.

In order to ensure the real time and accuracy of the mapping table, when the power system data dynamic changes, the mapping table must be updated timely and dynamically.

We adopt the method of setting up time stamp. The establishment of timestamp K_i , it express the time interval of the historical time and the current data acquisition time. If $\Delta t = t_1 - t_0$ is less than K_i , the mapping B table will unchanged, if the model timer $\Delta t = t_1 - t_0$ is greater than K_i , the table will update and re initialization algorithm, that implement the automatic update of the mapping table.

C. Determine the Sensitivity Matrix A of the Interaction Effects between Information Attack and Physical Attack

The methods by the attacker selected to attack the power CPS are often diversity [9], therefore, for the analysis of the current attack path, a single analysis of information or physical risk factors is far from enough [10]. This paper presents the sensitivity matrix of the interaction effects between information attack and physical attack to resolve attack path characteristics issues [11].

TABLE III: ATTACK METHOD TRANSFORMATION

attack method number	attack method conversion relationship	attack sensitivity
I1	I1→I1/I1→I4/I1→I8	0.17/0.34/0.59
I2	I2→I2/I2→I3	0.74/0.26
I3	I3→I3/I3→I9/I3→E1/ I3→E2/I3→E5	0.26/0.44/0.11/ 0.12/0.07
I4	I4→I4/I4→I7/I4→I8/I4→I9	0.11/0.12/0.09/0.08
	I4→E5/I4→E7/I4→E3/	0.2/0.04/0.16/
	I4→E2/I4→E4	0.15/0.05
I5	I5→I5/I5→I9/I5→E2/ I5→E5	0.35/0.42/0.21/0.02
I6	I6→I6/I6→I3/I6→I8/ I6→E1	0.28/0.16/0.5/0.06
I7	I7→I7/I7→I1/I7→I3/	0.26/0.34/0.14/
	I7→I4/I7→I8/I7→E2	0.16/0.03/0.07
I8	I8→I8/I8→I2/I8→I3/I8→I4/	0.19/0.13/0.21/0.07/
	I8→E2/I8→E8/I8→E3	0.09/0.24/0.07
I9	I9→I9/I9→I5/I9→E1/	0.21/0.18/0.23/0.14/
	I9→E2/I9→E4	0.19/0.05
E1	E1→E1/E1→E2/E1→I1	0.33/0.57/0.1
E2	E2→E2/E2→E3/E2→E4/	0.12/0.25/0.34/
	E2→E5/E2→E6/E2→I1	0.17/0.07/0.05
E3	E3→E3/E3→E4/E3→E6	0.36/0.35/0.29
E4	E4→E4/E4→E5/E4→E6	0.17/0.16/0.31
	/E4→E9	/0.26
E5	E5→E5/E5→E7/E5→E8	0.34/0.3/0.36
E6	E6→E6/E6→E7/E6→E8	0.18/0.25/0.21
	/E6→E9	/0.36
E7	E7→E7/E7→E8/E7→E9	0.39/0.34/0.27
E8	E8→E8/E8→E6/E8→E7	0.04/0.09/0.57
	/E8→E9/E8→I8	/0.24/0.06
E9	E9→E9/E9→E6	0.87/0.23

Due to the problem of solving the sensitivity matrix can be abstracted into HMM state transition matrix to solve the problem [12], so we use the Forward-Backward algorithm to calculate the sensitivity matrix in a time stamp [13]. It is very important to select the appropriate value in the initialization of the sensitivity matrix. According to the knowledge of the expert knowledge and experience, the initial sensitivity table is sorted out, as shown in Table III.

The initialization of the interaction sensitivity matrix A can be calculated through importing Table III, among $\mathbf{A} = \{a_{ij}\}$, row vector and column vector are all represent the number of attack method. After the completion of the initial matrix construction, it is necessary to carry out training A, the training process is as follows:

1) Pre sensitivity calculation before system attack

The sensitivity of the system before the attack indicates that the *t* moments are satisfied with the attack state X_i, and the *a* moments (including the *t* moment) meet the probability of a given attack sequence $\{n_1, n_2, n_3, \cdots n_t\}$ determined by historical data. The calculation of sensitivity $P(N_t \mid \lambda)$ before the system attack need to pass two steps:

Step one: pre sensitivity initialization

$b_i(n_1)$ represents the probability of an attack state n_1 at the initial time result in the system failure.

Step two: the induction algorithm of the conditional probability.

By the results of pre initialization sensitivity, combined with the actual data of the power CPS, we can get the following formula by using Forward Algorithm, which can be used to find out the sensitivity of the system before the attack:

$$P(N_t \mid \lambda) = \sum_{i=1}^{N} \left\{ \left[\sum_{i=1}^{N} \alpha_t(i) a_{(i,j)} \right] \cdot b_j(n_{t+1}) \right\} \quad (1)$$

2) Post sensitivity calculation after system attack

With similar to the calculation of sensitivity before the system attack, the sensitivity of the system after the attack at time t meet the attack state X_i, and the probability of a given attack sequence $\{n_{t+1}, n_{t+2}, n_{t+3}, \cdots n_T\}$ determined by the historical data. The calculation of sensitivity $\beta_t(i)$ after the system attacks requires two steps:

Step one: set constraint conditions of post sensitivity

$$\sum_{i=1}^{T} \beta_T(i) = 1 \quad (2)$$

It represents the sum of the post sensitivity in each time is 1, that is to say, the sensitivity contains in the set of information physical attack sequence.

Step two: the induction algorithm of post sensitivity

$$\beta_t(i) = \sum_{j=1}^{N} a_{(i,j)} \cdot b_j(n_{t+1}) \cdot \beta_{t+1}(j) \quad (3)$$

3) The calculation of sensitivity matrix A

This probability is obtained by the pre sensitivity and post sensitivity.

$$a_{ij} = \frac{\alpha_t(i)a_{(i,j)}b_j(n_{t+1})\beta_{t+1}(j)}{P(N_T \mid \lambda)} = \frac{\alpha_t(i)a_{(i,j)}b_j(n_{t+1})\beta_{t+1}(j)}{\sum_{i=1}^{N}\left\{\left[\sum_{i=1}^{N}\alpha_t(i)a_{(i,j)}\right]\cdot b_j(n_{t+1})\right\}+\sum_{j=1}^{N}a_{(i,j)}\cdot b_j(n_{t+1})\cdot\beta_{t+1}(j)} \quad (4)$$

IV. Implementation Algorithm of Attack Path Extraction Model in Power CPS

According to the model architecture is constructed as shown in Fig. 2, the model inputs are the original state monitoring sequence produced in IDS and EMS system. Through the determination of model parameter, and model solving process, the outputs are the attack path that the attackers are most likely to take. The entire solution algorithm is divided into the following four stages:

IN: the state monitoring sequence in IDS and EMS

OUT: attack path $N=\{n_1,n_2,n_3,\cdots\cdots n_{\max N}\}$

Step 1 System failure joint sequence acquired *M*

1) The IDS data is represented by IS set sequence

IS={T, IP, Hostname, M, Event, Sig_name, Sig_pri}

2) The EMS data is represented by OS set sequence

OS={T, StationName, M, Device, Value, Exception_type};

3) If the IS match filter conditions, then the IS= information system failure sequence subset;

4) If OS matches filtering conditions, then the OS= power system failure sequence subset;

5) Information system failure sequence subset are segmented according to the IP attribute, getting IS_n;

6) Power system failure sequence subset are segmented according to the StationName attribute, getting OS_m;

7) if $\forall t_i < t_j < t_{i+n}$ or $\forall\left|t_{j+m}-t_{i+n}\right| < t_d$, IS_n and OS_m merge sort, get System failure joint sequence *M*

8) else return "input failed to re gain"

Step 2 Determine the probability matrix of system failure B

1) Create mapping table between information physics cooperative attack and system failure

2) Calculation of the probability matrix of system failure B

3) Set up a program timer

4) if $\Delta t \le K_i$ then no need to update the mapping table

else update the mapping table and re calculate the probability matrix of failure.

Step 3 Determine the sensitivity matrix of the interaction A

1) Initialize $\pi=\left(\frac{1}{n},\frac{1}{n},\frac{1}{n},\cdots\frac{1}{n}\right)$

2) Give initial A and B, initialize $a_l(i)=\pi_i\cdot b_i(n_l)$

3) Calculate $P(N_t \mid \lambda)$, when the initial λ parameters, at t moment of the pre sensitivity

4) Calculate the probability sensitivity $\beta_t(i)$, at the t+1 moment to the end of the sequence

5) According to the results of the first two steps to get $\mathbf{A}=\{a_{ij}\}$

Step 4 The solution of attack path extraction

1) Get the π, **A**, **B**, M according to the above steps

2) While (t<T) {

if t=1 then $\delta_1(i)=\pi(i)b_{im_1}$

else

$$P(N_t)=\max_{i=n_1,n_2\cdots n_n}=P(N_{t-1})*P(A_{ij})*P(O_t \mid i)=\max_j(\delta_{t-1}(j)a_{ji}b_{iO_t})$$

$$N(i)=\arg\max\left(P(N_t)\right)$$

t++ }

end

Step 5 Traceback

$N_t=\psi_{t+1}(N_{t+1}) \quad t=T-1,T-2,\cdots T$

Since the Vitby algorithm [17]-[19] to save the best path for the $P(N_t)$, so the traceback from the final state can be pushed back, thus forming the maximum probability of attack path *N*.

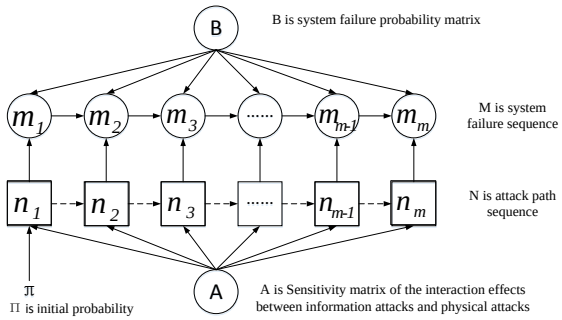

Fig. 2. Attack path extraction model of power CPS

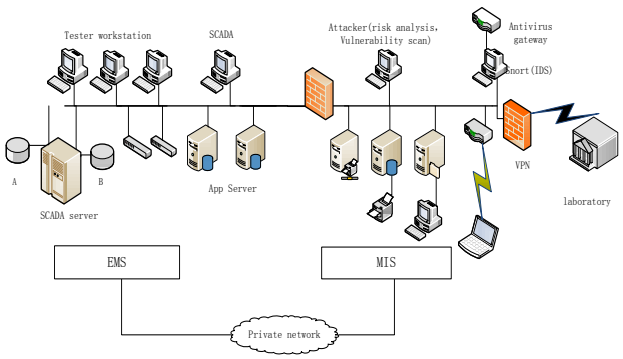

Fig. 3. Attack experiment simulation environment

V. Attack Path Extraction Example Analysis

In order to verify the effect of attack path extraction model, we design and set up an attack experiment simulation environment, as shown in Fig. 3. The environment include Snort system (open source IDS system), it be used to collect all kinds of analog information of attack warning and system failure results. At the same time, we obtained 7 days EMS system data

from the actual power operation in a provincial electric power company, the data include telemetry, remote communication and information statistics [14]. Through the data playback technology to achieve all the running state of the EMS history data playback, we simulate the attacker tamper with the control instruction and state information, or implement all kinds of physical attacks [15]. We record all kinds of system failure sequence in the attack process [16].

In the experimental environment, the information attack and physical attack are used to combine the cooperative attack method. The sum of simulated and attacked is 15 times. The experiment mainly includes 3 stages:

Stage 1: Launch information physical cooperative attack. The attack sequence such as I3-E1-E3 (attack means in the Table I, the actual sequence of the attack path in the Table II), the sequence length from the 3 step to the 6 step.

Stage 2: System failure sequence acquired. According to the original monitoring state sequence in the IDS and EMS, the joint system failure sequence were obtained through the filtering, segmentation and fusion processing, (the system failure sequence in the Table IV).

Stage 3: Attack path extraction. According to the table 2 and table 3, respectively, the system failure probability matrix B and interactive impact sensitivity matrix A is determined. Based on these parameters, the model of attack path extraction built to calculate the possible attack path (see Table IV for extracting attack path).

TABLE IV: EXPERIMENT OF ATTACK PATH EXTRACTION

No	Actual attack path	System fault sequence	Extract attack path
1	I3-E1-E3	F8-F1-F2	I3-E1-E3
2	I3-E2-E7	F8-F1-F2	I3-E2-E6
3	I4-E2-E7	F9-F1-F4	I3-E2-E7
4	I2-E4-E2	F10-F2-F5	I2-E4-E2
5	I8-I5-E1	F11-F9-F7	I8-I5-E1
6	I7-E2-E7-E6	F8-F1-F4-F3	I7-E2-E7-E6
7	I7-I4-E3-E9	F8-F9-F2-F3	I7-I4-E3-E9
8	I5-I8-E1-E4	F9-F11-F4-F5	I5-I8-E1-E3
9	I2-E4-E5-E2	F10-F5-F6-F7	I2-E4-E5-E2
10	I4-E4-E8-E5	F12-F2-F4-F6	I4-E4-E8-E6
11	I3-E2-E7-E4-E5	F8-F1-F2-F5-F6	I3-E2-E7-E4-E5
12	I4-E4-E5-E2-E7	F9-F2-F3-F5-F2	I4-E7-E5-E3-E7
13	I8-E2-E3-E4-E7	F11-F1-F2-F3-F4	I8-E1-E3-E4-E7
14	I4-E2-E9-E3-E6-E5	F9-F1-F2-F5-F6-F7	I4-E2-E5-E3-E9-E5
15	I8-E3-E5-E7-E2-E6	F11-F2-F3-F4-F5-F6	I8-E3-E6-E7-E1-E6

Note: A border attack method means that the extraction of attack path is error.

According to the data on Table IV, web graph of the relationship between the transformation of the attack method is constructed. Two strong correlation attacks (E2-E5-E7，I2-E4) can be found in the graph, as shown in Fig. 4

Fig. 5 shows that, with the increase of the attack sequence length, the accuracy of the extraction path shows a downward trend, the accuracy rate of extraction path reached 86.7% in the 3 step attack sequence. The accuracy of the extraction path is basically the same in the 4 step and the 5 step attack sequence, which is 90.2% and 81.4% respectively, when the 6 step is reached 66.7%.

The main reasons for the change are as following: At first, with the increase of the attack sequence length, the attack target and the means by the attacker used are more and more obvious. Therefore, the accuracy of the extraction path is also promoted. But when the attack sequence reaches a certain length, the probability of the attacker's target transfer is increased. It is possible to be mixed with different attempts to attack in the sequences, this is the reason for the decline in the accuracy of attack sequence extraction.

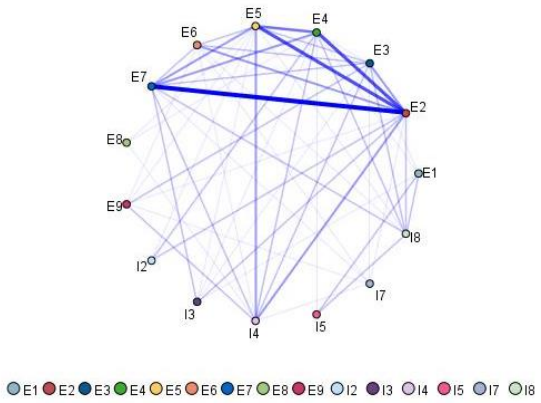

Fig. 4. Relationship between the transformation of the attack method

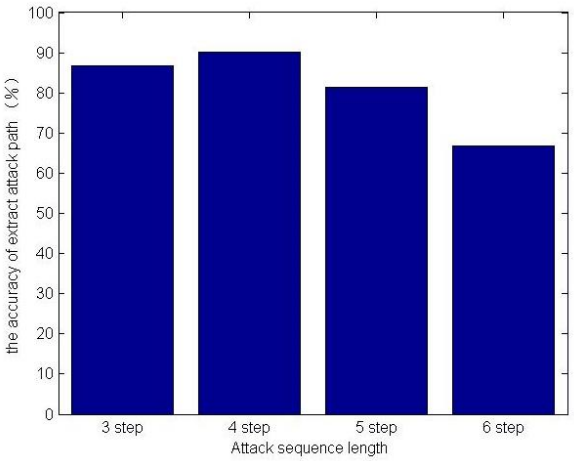

Fig. 5. Accuracy rate of attack path extraction

VI. CONCLUSIONS

With the deep integration of power information system and physical system, the new cooperative attack mode has brought serious challenges to the security and stability of power system. This paper proposed an attack path extraction model based on HMM in power CPS, the model can automatic extract the most likely attack strike path, according to the change of the system failure state sequence.

The extraction model of attack path only considers the correlation of the adjacent two attacks, it can't deal with the complex multi-step cross attack which exist in the actual attack. The aim of this paper is to explore the model and method of cooperative attack path analysis. In the next step, the plan is designed to use big data processing method in feature extraction and the risk assessment of power CPS.

REFERENCES

[1] Q. L. Guo, S. J. Xin, J. H. Wang, and H. B. Sun. "Comprehensive security assessment for a cyber physical energy system: A lesson from ukraines blackou," *Automation of Electric Power Systems*, vol. 40, no. 5, pp. 145-147, May 2016.

[2] X. Y. Tong and X. R. Wang, "Inference and countermeasure presupposition of network attack in incident on ukrainian power grid," *Automation of Electric Power Systems*, vol. 40, no. 5, pp. 144-148, Jul. 2016.

[3] N. Liu and J. H. Zhang, "Coordinated cyber-attack: Inference and thinking of incident on ukrainian," *Power Grid. Automation of Electric Power Systems*, vol. 40, no. 6, pp. 144-147, Jun. 2016.

[4] Y. Wang, X. S. Han, D. Ying, and S. Jie, "Markov chain-based rapid assessment on operational reliability of power grid," *Power System Technology*, vol. 37, no. 2, pp. 137-141, Oct. 2006.

[5] Y. Q. Wang and F. C. Lu, "Synthetic fault diagnosis method of power transformer based on rough set theory and bayesian network," *Proceedings of the CSEE*, vol. 33, no. 10, pp. 405-410, Feb. 2013.

[6] J. H. Zhao, F. S. Wen, and Y. S. Xue, "Modeling analysis and control framework physical power information fusion system," *Automation of Electric Power Systems*, vol. 35, no. 16, pp. 1-8, May 2011.

[7] Y. Tang, Q. Wang, and N. Ming, "Electricity networks physical attack information fusion system," *Automation of Electric Power Systems*, vol. 40, no. 6, pp. 148-151, Jun. 2016.

[8] J. D. Cai and R. W. Yan "ARMA bispectrum analysis and discrete hidden markov model in power electronic circuit fault diagnosis," *Proceedings of the CSEE*, vol. 30, no. 24, pp. 54-60, May 2010.

[9] G. S. Liu, C. L. Zhang, and X. Yue, "HMM viterbi algorithm based on inverse system than the theory of algorithms," *Electrical Engineering Technology*, vol. 43, no. 11, pp. 7-10, Nov. 2014.

[10] Q. L. Guo, S. J. Xin, H. B. Sun, and J. Wang, "Fusion power system modeling and information about the physical safety assessment: The driving force and vision research," *Proceedings of the CSEE*, vol. 36, no. 6, pp. 1481-1489, Jun. 2016.

[11] Q. Wang, F. S. Wen, and J. H. Li, "Risk-Based security-constrained economic dispatch in power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 23, no. 5,pp. 142-149, May 2013.

[12] J. X. Wang, H. W. Zhong, Q. Xia, and C. Q. Kang, "Transmission network expansion planning with embedded constraints of short circuit currents and N-1 security," *Journal of Modern Power Systems and Clean Energy*, vol. 33, no. 6, pp. 312-320, Jun. 2015.

[13] Y. Q. Wang, F. C. Lu, and M. Li, "Synthetic fault diagnosis method of power transformer based on rough set theory and bayesian network," *Proceedings of the CSEE*, vol. 14, no. 8, pp. 137-141, Apr. 2006.

[14] C. Y. Qu, Q Yang, J. M. Yang, W. Q. Liu, and N. Qu "Risk associated model of intelligent substation based on bayesian network," *Automation of Electric Power Systems*, vol. 40, no. 2, pp. 95-99, Jan. 2016.

[15] L. J. Chen and X. Z. Hu "2008 national transmission reliability analysis," *China Electric Power*, vol. 42, no. 5, pp. 1-6, May 2009.

[16] I. Votsi, N. Limnios, and G. Tsaklidis, "Papadimitriou. Hidden Markov models revealing the stress field underlying the earthquake generation," *Physica A: Statistical Mechanics and its Applications*, vol. 13, no. 6, pp. 21-24, Jun. 2013.

Lei Wang was born in Jilin Province, China in 1979. He is pursing his Doctor's degree of electrical engineering in the School of Electrical Engineering Northeast Dianli University. His research interests is information processing in Smart grid. His e-mail is neduwanglei@qq.com.

Zhaoyang Qu was born in Jilin Province, China in 1964. He received his Doctor's degree of electrical engineering in 2010 from North China Electric Power University, Baoding. Currently he is professor in the School of Information Engineering of Northeast Dianli University. His research interests include intelligent information processing, virtual reality, and computer network.

Zelong Li was born in Heilongjiang Province, China in 1989. He received his Bachelor's degree of business management in 2013 from Anhui University. His research interests include intelligent information processing, virtual reality, and computer network. His e-mail is 531146846@qq.com