Fuzzy Comprehensive Evaluation Algorithm for Power Information System Security Level Based on the Internet of Things

http://dx.doi.org/10.3991/ijoe.v12i05.5730

Zeng Ming and Wang Shicheng
North China Electric Power University, Beijing, China

***Abstract*—With the development of information and communications technology, communication technology has been widely used in the electric power industry and has brought threats to the safe operation of power systems. Things can not only connect people; things can also connect other things. Therefore, the Internet of things plays an important role in power information system security. This study proposes a triangular fuzzy number weight method to calculate the index weight based on the analysis of the existing fuzzy algorithm and the security of a power information system. A fuzzy comprehensive evaluation model is established in accordance with matrix theory, statistical theory, and other methods after experimental data are analyzed. Results show that this algorithm can accurately evaluate system status and provide reference for managing power systems. The fuzzy algorithm for power information system security level ensures the safe operation of the power system and promotes its healthy development. This algorithm can significantly promote economic development in China.**

***Index Terms*—Electric power information system, Fuzzy algorithm, Internet of things**

I. INTRODUCTION

With the rapid development of information and communications technology in recent years, the information network has penetrated into every corner of society. Accordingly, information security has gained increasing attention. The safe operation of a power system depends on information system security, which promotes research on information security issues in the power industry. The study of the security of an electric power information system is important for the development of the power industry to ensure the smooth progress of the socialist construction [1]. Power information systems experience increasing incidents of deception and network attacks. The original security system is prone to new hidden security dangers. Electric power information systems even pose a new threat to power systems themselves. Current network protocols and security mechanisms have natural defects. Management and policy makers should consider security issues. The system is not sufficiently perfect; major accidents frequently happen. Its political influence is significant, and the economic loss incurred by electric power enterprises is immeasurable. Information on power system security, including network security, secure delivery, security policy formulation, and management methods, requires in-depth analysis. To explore the establishment of a power information system security model, strengthening power system security will provide thousands of long-term services [2].

With the rapid development of information technology worldwide, information security incidents have emerged in an endless stream. They have brought considerable losses and have seriously hindered the healthy development of information technology. For example, in November 1988, a Cornell graduate student, Robert Morris, released the computer worm (now known as the Morris worm), which affected approximately 60000000 online computers in Taiwan. The corresponding loss was initially estimated to be approximately US$100 million. Vladimir Levis and his allies in Russia intruded into the cash management system of Citibank in June 1994 and transferred a huge amount of money into their own bank account in another bank. By the time of his arrest, he hadcollected over US$500 million. During the 1980s and 1990s, Kevin Mitnick cloned cellular phone systems, such as Motorola, Novell, and Fujitsu, as well as various computer systems, such as Microsystems and Sun. The Federal Bureau of Investigation arrested him for telecommunications, computer, and wired frauds, and he was sentenced to 46 months in prison. In July 1996, Timothy Lloyd, a New Jersey program design engineer for Omega, was fired for unleashing the “time bomb” software, which deleted all the work plan of the company. He was eventually sentenced to 41 months in prison, with a compensation amounting to US$2 million. In July 1996, Jester, a teenage hacker, illegally accessed the NYNEX business cycle and sent a series of instructions to the carrier system, which disabled the services of the Federal Aviation Administration control tower, the Worcester Airport, and the entire Massachusetts, Rutland for 6 h. In February 1998, two boys from California, as directed by a military adviser in Israel, intruded into the system of the United States. During that time, the relationship between Iraq and the United States had deteriorated, and the intrusion nearly led to a national military conflict between the United States and Arabia. In March 1993, David Smith released the Melissa virus, which affected approximately 1000000 Taiwan computers and caused a loss of approximately US$8000. Onel de Guzman from the Philippines launched the “I LOVE YOU” virus in May 2000. This virus infected 45000000 computers worldwide, which caused estimated losses of US$10 billion. In July 2001, the Code-Red worm affected computers running Microsoft’s Internet Information Services web server. Buffer overflow vulnerabilities occurred, which infected 350000 computers and resulted in losses of over US$2 billion.

The development of information technology in China is relatively backward. Meanwhile, information security incidents in developed countries are serious, and the overall situation remains pessimistic. Information security consciousness in China is lagging behind. In April 1998, a college student from southern China collected information on the Internet regarding national defense scientific research and showed it to the Yangcheng Evening News, which published it in < >. The survey found thousands of articles related to military confidential information. In September 1998, two brothers, Hao Jinglong and Hao Jingwen, attacked the computer system of a bank and stole 260000 yuan. A serious leak occurred in 1999. During that time, an engineer published a column in Education Online. According to a national survey in the 1990s, 70% to 80% of 40 million computers are infected with viruses, and over 6% of computers contain a Trojan [3].

With the development of international information security, the information security standards in China are also advancing. China has learned from a number of successful experiences from foreign information security policies and regulations. The corresponding gains and losses that conform to the situation of the country are considered. China has initially established a national information security guarantee system. The State Council Information Office established a special leading group of network and information security. Provinces, municipalities, and autonomous prefectures also have a corresponding management mechanism [4].

The remainder of this paper is organized as follows. Section 2 presents the problem. Section 3 provides the technical description of the process. Section 4 describes the data analysis. Section 5 concludes the study.

II. STATE OF THE ART

A. Basis of the Internet of Things (IOT)

IOT refers to access to information through all types of terminal equipment, all types of information acquisition technology, the Internet, telecommunication networks, and other information carrier networks. Its objective is centralized access to information. Instructions are transmitted to terminal equipment to realize intelligent control of equipment. IOT terminal information collection technologies include radio frequency identification (RFID), sensors, video recognition, infrared identification, 2D barcode-scanning, GPS, and laser. These technologies can automatically access various information.

The concept of IOT was first proposed in 1999 to add terminal equipment to the Internet or extend Internet applications. The IOT concept was presented at the 2005 World Summit on the Information Society by the International Telecommunication Union (ITU). The ITU reported that the coverage of IOT will be expanded and it will no longer be limited to RFID technology [5].

IOT exhibits the following three basic characteristics: overall perception, namely, the use of various sensor and identification technologies to obtain information regarding an object at any time; reliable transmission of electricity via a communication network, i.e., other means of communication resources, if necessary, and accurate information about the object sent to the destination; intelligent processing of massive amounts of data and information analysis and processing, i.e., the object implementation of intelligent control. In general, IOT includes the perception, network, and application layers. The IOT model is shown in Figure 1.

Figure 1. IOT model

The Massachusetts Institute of Technology proposed the concept of networking in 1999; wireless data communication technology was connected to the Internet to achieve intelligent recognition and control [6]. Accordingly, things based on the Internet were expanded and extended. We cannot simply regard IOT as an extension of the Internet. IOT is also a type of intelligent applications. Sound, light, electricity, temperature, and other information are connected and exchanged through terminal equipment. Information is analyzed and processed by controlling several terminals to achieve intelligent processing. The combination of various modern network technology, sensing technology, artificial intelligence, and automation technology realizes human–object dialogue to create a world of wisdom.

B. Application of the Power Network of Things

The power of networking refers to the formation of a large intelligent network that comprises power system equipment and people using sensor information through networks and database technology. The power of networking has the following functions: system identification of various types of electrical equipment, evaluation of the “healthy” state of power system equipment, electric quantity monitoring of the network nodes of a power system, maintenance or operating personnel implementation of real-time tracking, and information processing by technical personnel [7]. The platform structure of electric power and IOT is illustrated in Figure 2.

(1) Saving energy and reducing consumption

A sensor has a watt–hour meter; hence, the power supply department can keep track of the electricity used at any time to realize efficient energy management and achieve the goal of energy conservation.

(2) Improving running equipment safety and reliability

Real-time monitoring of equipment is implemented, the running status of equipment is identified, and the security and reliability of equipment operation are improved.

(3) Improving the working efficiency and ensuring the security of the staff

Staff members are equipped with an RFID device to track them in real time when they are working. This approach does not only can promote the work efficiency of employees but also ensures their safety.

(4) Ensuring the recovery and utilization of instruments and tools

The IOT system allows automatic registration and tracking of instruments and tools, thereby preventing the loss and theft of instruments. Instruments and tools are also used to supervise staff.

(5) Promoting the application of a"paperless" organization

The IOT system records and tracks the management of electrical equipment through an automatic system, which changes the manual recording in papers prevalent in the past and achieves the goal of a "paperless" organization. IOT technology is suitable for safety management and for realizing paperless online management of staff members and instruments.

System administrators connect to the network server by logging into a computer with their user name and password. Consequently, they can monitor sites and the state of the power system in real time [9]. The power quality safety analyzer is shown in Figure 3.

III. METHODOLOGY

Power is an important part of the daily lives of people and helps safeguard economic development. The development of electric power informatization and power systems is constantly moving forward. An electric power information system includes link power generation, transmission, distribution, and power supply monitoring, and thus, ensuring the security of an electric power information system is critical. However, security problems, such as viruses and Trojans, ceaselessly emerge in electric power information systems. The problem of system security cannot be solved by simply relying on technology. An advanced security evaluation level of electric power information systems, an evaluation of the running status of electric power information systems, and the timely discovery of security vulnerabilities and risks are required. Accordingly, this study adopts the improved analytic hierarchy process (AHP) to establish a fuzzy comprehensive evaluation model for electric power information systems.

A. *AHP*

AHP is a quantitative analysis and decision-making method for fuzzy complex problems. This method can be used in the evaluation process to determine the index weight. The basic principle of this algorithm is used to determine the index weight through the comprehensive analysis of safety factors. These factors may be interconnected or independent of one another. They are organized in a hierarchical structure according to the subordinate relations among them. The importance of two factors is compared by constructing a judgment matrix. The judgment matrix is then solved based on the corresponding eigenvector matrix to calculate the relative weights of each factor. The concrete steps are as follows.

(1). A hierarchy model is constructed. The problem is carefully analyzed. Target factors are divided into several levels according to the different attributes of various factors.

(2). A comparison matrix is constructed. Importance indices are compared from the second to the last layer in the hierarchical structure, and two discriminant scales are set based on the given structure judgment matrix.

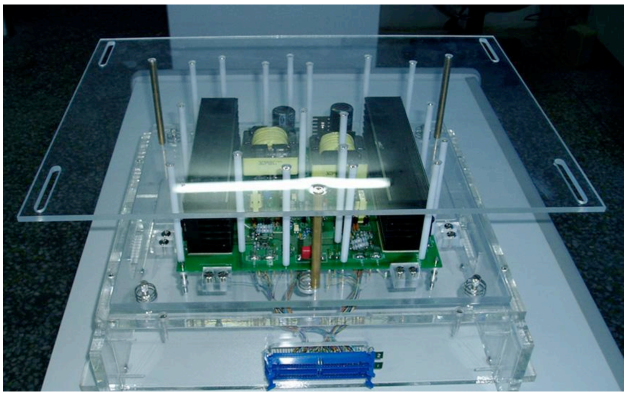

Figure 2. Platform design structure

Figure 3. Power quality safety analyzer

(3). The consistency of the judgment matrix is tested and calculated using the formula for the consistency index.

(4). The weight of the factors are determined.

AHP is applied to evaluate the index weight during the calculation process. This method is simple and practical. The combination of qualitative analysis, quantitative analysis, and the human hierarchical thinking process simplifies the tedious problem. However, AHP has certain disadvantages in determining the judging matrix of the evaluation index. Various experts have different subjective preferences; hence, the objectivity of the results is not guaranteed. The comprehensiveness of knowledge is also uncertain.

B. *Fuzzy Comprehensive Evaluation Algorithm*

The main objective of fuzzy mathematics is to target fuzziness in real situations. Fuzziness refers to the uncertain characteristic of an object, namely, "also." Fuzzy theory was published in the United States in 1965. Its specific definition, related theory, membership degree, and fuzzy set are introduced to represent the meaning of numerical values. The traditional mathematical description of a phenomenon is true or false. Fuzzy theory can help understand and solve this problem. The related concepts of fuzzy theory used in this study are provided in detail.

A fuzzy comprehensive evaluation model is established using matrix theory, the calculation method of statistics, and other theories that deal with multiple factors.

(1). The evaluation factor set U for power information system security is constructed.

(2). Set V is determined.

(3). A single-factor judgment matrix is established. V corresponds to a fuzzy set of the process, which is actually built from u to V of a fuzzy mapping. Fuzzy mappings can obtain a fuzzy judgment matrix and a fuzzy evaluation matrix R.

(4). First-level fuzzy comprehensive evaluation is conducted. The weight of each index is used for reference, and the fuzzy set of the upper level factor is obtained based on the fuzzy judgment matrix in step 3.

$$B_i = (\sum_{i=1}^{n} w_i r_{i1}, \sum_{i=1}^{n} w_i r_{i2}, \dots \sum_{i=1}^{n} w_i r_{im}) \quad (1)$$

5. A two-level fuzzy comprehensive evaluation is performed. The final evaluation results of the final target layer can be obtained based on the first-level evaluation results in step 4 (Figure 2).

$$B = (\sum_{i=1}^{s} c_i . l_{i1}, \sum_{i=1}^{s} c_i . l_{i2}, \dots, \sum_{i=1}^{s} c_i . l_{im}) \quad (2)$$

From Formula 1, we can conduct a comprehensive evaluation, hardware security evaluation, network security evaluation, information security evaluation, and software security evaluation. Similar to Formulas 3–6, Formula 2 indicates that we can generate two comprehensive evaluations from Formula 7.

$$B_1 = w_1 \times R_1 \quad (3)$$

$$B_2 = w_2 \times R_2 \quad (4)$$

$$B_3 = w_3 \times R_3 \quad (5)$$

$$B_4 = w_4 \times R_4 \quad (6)$$

$$B = w \times \begin{bmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{bmatrix} \quad (7)$$

From the preceding security analysis of an electric power information system, an information security level evaluation index system is established. The triangular fuzzy number weight calculation method is used. The established fuzzy comprehensive evaluation model for power information system safety is applied. According to the preceding formulas, we can conduct security situation assessment [10].

IV. RESULT ANALYSIS AND DISCUSSION

The threat degree of security attacks can be classified into high and low grades, i.e., 3, 2, and 1. The threat severity degrees of some of these attacks are provided in Table I.

The Lincoln Laboratory of the Massachusetts Institute of Technology constructed a Defense Advanced Research Projects Agency data set for experimental data in 1999. Data include the network boundary, the network data information, the real attack data set (see Table II), and the Windows NT audit log (Hu et al. 2013) [9]. Alarm information and audit log are combined. The attack data are collected from Monday to Friday at 8:00 to 23:00 in accordance with the proposed model for the situation assessment calculation of network security situation value (Figure 4).

The experimental results show that compared with other algorithms, the proposed algorithm can more accurately predict the network security situation.

TABLE I.
PART OF THE ATTACK CATEGORY AND THREAT DEGREE MEASUREMENT

Hit class	Description	Threat degree
Unsuccessful user	Attempt to obtain user rights	3
Attempted admin	Attempt to obtain administrator privileges	3
Detected Trojan	Detect Trojan	3
RPC port-map decode	Remote procedure call query decoding	2
Attempted DOS	Attempted denial of service	2
Network scan	Network scan detection	1

TABLE II.
NT WINDOW HOST PART OF THE ATTACK RECORDS

Source address	Destination address	Detection time	Hit class
172.016.118.070	172.016.112.100	41.16.13	Yaga
172.016.118.070	172.016.112.100	41.19.50	Yaga
172.016.118.070	172.016.112.100	41.20.13	Crashiis
205.160.208.190	172.016.112.100	42.14.32	Sechole
209.001.012.046	172.016.112.100	42.21.04	Crashiis
….			

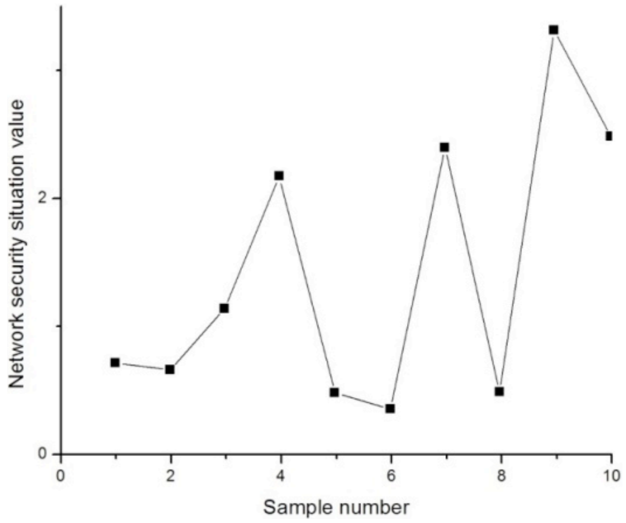

Figure 4. NT Windows host security situation

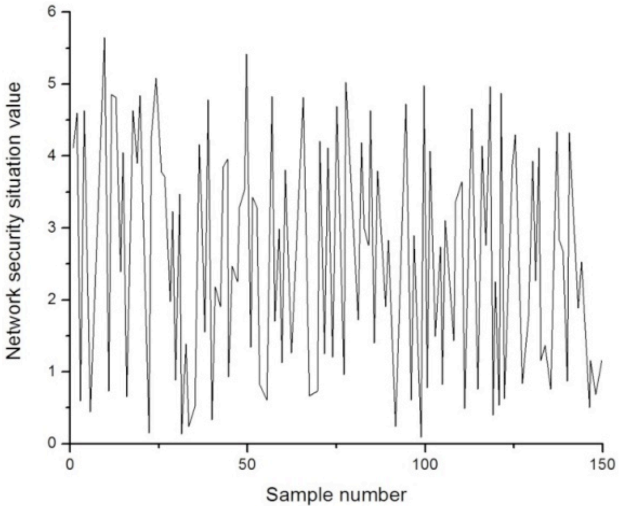

Figure 5. Network security situation curve

V. CONCLUSIONS

With the development of information technology, network security has attracted attention. A close relationship exists between power systems and the lives of people. Accordingly, the safety of power systems is particularly important. The safe application of networking technology can effectively improve data security and operation. The current networking power of information security technology is analyzed by focusing on the shortcomings of the fuzzy comprehensive evaluation model for data processing using several mathematical models. The evaluation results indicate that the proposed method can accurately monitor the network security situation. Studying the security problem of electric power information systems based on IOT technology is important to promote the development of electric power information systems.

REFERENCES

[1] Jamuary, Nur Atika, et al., "Contributing Factors of Online Brand Trust in Airline Industry," *Advanced Science Letters*, 2015, vol. 21, no. 10, pp. 3395-3398. http://dx.doi.org/10.1166/asl.2015.6524

[2] Abilock, Rigele, and Debbie Abilock., "i agree, but do i Know? Privacy and Student Data," *Knowledge Quest*, 2016, vol. 44, no. 4, pp. 10.

[3] Bray, Marty, "Going Google: Privacy Considerations in a Connected World," *Knowledge Quest*, 2016, vol. 44, no. 4, pp. 36.

[4] Mazurczyk W, Caviglione L., "Steganography in modern smartphones and mitigation techniques," *Communications Surveys & Tutorials, IEEE*, 2015, vol. 17, no. 1, pp. 334-357. http://dx.doi.org/10.1109/COMST.2014.2350994

[5] Kozachenko, D., R. Korobyova, and R. Rustamov, "Improving of technical means and technologies of grain transportation for export in Ukraine," *News of Dnipropetrovsk State Agrarian and Economic University*,2015, vol. 4, pp. C-121.

[6] Guériau, Maxime, et al., "How to assess the benefits of connected vehicles? A simulation framework for the design of cooperative traffic management strategies," *Transportation Research Part C: Emerging Technologies,* 2016, vol. 67, pp. 266-279. http://dx.doi.org/10.1016/j.trc.2016.01.020

[7] Gonder, Jeffrey, Eric Wood, and Sai Rajagopalan, "Connectivity-Enhanced Route Selection and Adaptive Control for the Chevrolet Volt," *Journal of Traffic and Transportation Engineering,* 2016, vol. 4, pp. 49-60.

[8] Arnold, George., "Intelligent Systems: A New Industrial Revolution [Viewpoint]," *IEEE Electrification Magazine*, 2016, vol. 4, no. 1, pp. 64-63. http://dx.doi.org/10.1109/MELE.2015.2509904

[9] Liu, Sylvia Xihui., "Innovation Design: Made in China 2025," *Design Management Review*, 2016, vol. 27, no. 1, pp. 52-58.

[10] Mourtzis, Dimitris, et al., "Cloud-based adaptive process planning considering availability and capabilities of machine tools," *Journal of Manufacturing Systems*, 2016, vol. 39, pp. 1-8. http://dx.doi.org/10.1016/j.jmsy.2016.01.003

AUTHORS

Zeng Ming is with the School of Economy and Administration, North China Electric Power University, Beijing 102206, China (e-mail: 18511791668@ 139.com).

Wang Shicheng (corresponding author) is with the School of Economy and Administration, North China Electric Power University, Beijing 102206, China (e-mail: shicheng_ wang @ 163. com).

Submitted, 09 March 2015. Published as resubmitted by the authors on 09 April 2015.