EAI Endorsed Transactions
on Scalable Information Systems

Research Article EAI.EU

Analysis and Design of Power System Transformer Standard Based on Knowledge Graph

Yuzhong Zhou[1,*], Zhengping Lin[1], Yuan La[2], Junkai Huang[3], and Xin Wang[1]

[1]Electric Power Research Institute of China Southern Power Grid Company (e-mail: yuzhong_zhou@hotmail.com, zhengping_lin@hotmail.com, xinwangcsg@hotmail.com).
[2]China Southern Power Grid Company Limited (e-mail: yuanlacsg@hotmail.com).
[3]Electric Power Research Institute of Guizhou Power Grid Co. , Ltd (e-mail: junkaihuangcsg@hotmail.com).

Abstract

The transformer can convert one kind of electric energy such as AC current and AC voltage into another kind of electric energy with the same frequency. Knowledge graph (KG) can describe various entities and concepts in the real world and their relationships, and it can be considered as a semantic network for power system transformer. Hence, it is of vital importance to analyze and design the power system transformer standard based on the knowledge graph. To this end, we firstly examine the power system transformer with one KG node and one eavesdropper E, where the eavesdropper E can overhear the network from the source, which may cause physical-layer secure issue and an outage probability event. To deal with the issue, we analyze and design the system secure performance under the eavesdropper and define the outage probability for system security, by providing analytical expression of outage probability. We further investigate the power system transformer with multiple KG nodes which can help strengthen the system security and reliability. For such a system, we analyze and design the system secure performance under the eavesdropper and define the outage probability for system security, by providing analytical expression of outage probability. Finally, we give some simulations to analyze the impact of secure transformer standard on the power system, and verify the accuracy of our proposed analytical expression for the the power system transformer standard based on the knowledge graph.

Received on 29 August 2022; accepted on 30 September 2022; published on 12 October 2022

Keywords: Power System, knowledge graph, analysis and design.

doi:10.4108/eetsis.v9i6.2642

1. Introduction

Transformer is a common electrical equipment, which can realize the conversion of AC energy. The transformer can convert one kind of electric energy (AC current and AC voltage) into another kind of electric energy (AC current and AC voltage with the same frequency) [1–3]. The function of transformer in practical application is mainly to complete the voltage conversion and make the transmission of electric energy more convenient. Transformers can be divided into step-down transformers and step-up transformers according to the ratio of output voltage to input voltage. A transformer whose ratio of output voltage to input voltage is less than 1 is called a step-down transformer [4]. Its main function is to provide the required voltage for various electrical equipment to ensure the supply of the voltage required by users. The transformer whose ratio of output voltage to input voltage is larger than 1 is called step-up transformer. Its main function is to reduce the power transmission cost, reduce the loss in the process of power transmission and increase the power transmission distance.

In case of the following changes of the transformer, the fault analysis of the transformer can be carried out according to the actual operation status of the transformer on site. During the operation of the transformer, an accident causes power failure or short circuit at the outlet, but it has not led to disassembly: the abnormal phenomenon of the transformer during

[*]Corresponding author. Email: yuzhong_zhou@hotmail.com

the operation forces the operator to conduct power outage maintenance and test on the transformer. During the preventive test, maintenance acceptance or handover of the transformer under normal power failure, one or more index values exceed the standard value. If any of the above conditions occurs during the practical use of the transformer, relevant inspection and test should be conducted immediately to ensure that the transformer can operate normally.

The steps of judging whether there is a fault are given as follows. First, we should identify the possibility of a fault in the transformer, and test whether the fault is an explicit fault or a hidden fault. Second, we should identify the nature of the fault, such as oil fault or solid insulation fault, thermal fault or electrical fault. Third, fault power, time, severity, development trend, hot spot temperature and saturation degree of gas in oil are common conditions to identify whether there is a fault in the transformer. Fourth, we should find a proper way to deal with transformer accidents. If the transformer can still operate after an accident, it is necessary to judge whether its safety technical measures and monitoring methods need internal inspection and repair during the operation of the transformer.

Transformer faults can be caused by various reasons, such as classification by type. For example, it can be divided into oil circuit fault, magnetic circuit fault and circuit fault according to its circuit division. At present, the probability of transformer fault is the highest, which is not only the short-circuit fault at the outlet of the transformer, but also the very serious impact on the transformer itself, and also the discharge fault of the transformer.

The main goal of knowledge graph (KG) is to describe various entities and concepts in the real world and their relationships. Therefore, it can be considered as a semantic network. From the perspective of development process [5, 6], knowledge graph is developed on the basis of natural language processing (NLP). Knowledge graph and NLP are closely related and belong to the top artificial intelligence (AI) technology. Knowledge graph can be used to query complex related information at a higher level, understand the user's intention from the semantic level, and improve the search quality. The application of knowledge graph technology provides a new perspective and idea for the design of power system transformer [7].

In this paper, we analyze and design the system secure performance under the eavesdropper and define the outage probability for system security, by providing analytical expression of outage probability. We further investigate the power system transformer with multiple KG nodes which can help strengthen the system security and reliability. For such a system, we analyze and design the system secure performance under the eavesdropper and define the outage probability for system security, by providing analytical expression of outage probability. Finally, we give some simulations to analyze the impact of secure transformer standard on the power system, and verify the accuracy of our proposed analytical expression for the the power system transformer standard based on the knowledge graph.

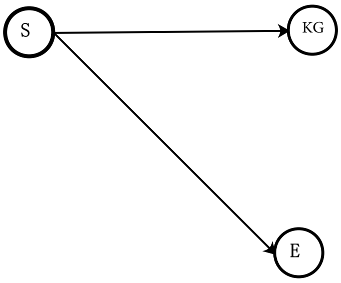

Figure 1. System model of the power system transformer standard based on knowledge graph with one KG node.

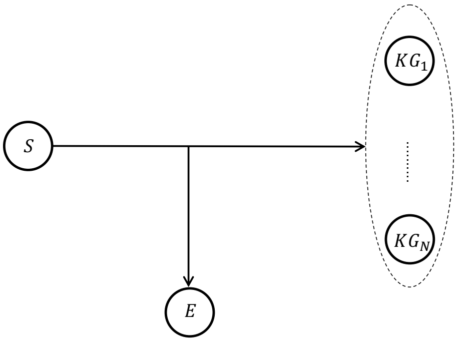

Figure 2. System model of the power system transformer standard based on knowledge graph with multiple KG nodes.

2. System model of power system transformer standard based on knowledge graph

2.1. One KG node

As shown in Fig. 1, we examine the power system transformer standard based on knowledge graph with a single KG node, where there exists a transmit source S, a receiver R receiving the signal, and one eavesdropper E. At each time slot t, the source S sends the signal to the receiver R, while the eavesdropper E can overhear the network from S to R, which may cause physical-layer security problems and an outage probability event. Let $h \sim \mathcal{CN}(0, \alpha)$ and $g \sim \mathcal{CN}(0, \beta)$ denote the wireless channel from S to R and from S to E, respectively. The transmission rate between S to R is given by [8]

$$C_{sr} = \log_2\left(1 + \frac{P}{\sigma^2}|h|^2\right), \tag{1}$$

where P is the transmit power, and σ^2 represents the variance of additive white Gaussian noise (AWGN) at the receiver. Analogously, the transmission rate from S to E is written as [9–11]

$$C_{se} = \log_2\left(1 + \frac{P}{\sigma^2}|g|^2\right). \tag{2}$$

For the considered network, the transmission security needs to be analyzed under the eavesdropper E, which can improve the system secure performance and the system effectiveness. Specifically, the outage probability event occurs when the eavesdropping transmission rate is larger than a certain threshold value of the transmission rate at the transmit source S. In the next subsection, we will give the definition of the outage probability and analysis the system security transmission performance.

2.2. Multiple KG nodes

Fig. 2 shows the system model of the power system transformer standard based on knowledge graph with multiple KG nodes. Specifically, the user can communicate with the KG nodes through the wireless link. At the same time, the eavesdropper can overhear the communication that can result in a reduction in the transmission rate. Without loss of generality, we assume that all nodes in this system have a single antenna and all links experience Rayleigh fading.

There are two communication cases in this network. One is that the user can communicate with all the KG nodes simultaneously, while the other is that the user can select one KG node to communicate. Since the former communication case may cause interference among the users and the user needs to have more antennas, the KG node selection technique is used in this paper. Specifically, we assume that the n^*-th KG node KG_{n^*} is selected to communicate with the user. Intuitively, we can select the best KG node KG_{n^*} by maximizing the instantaneous channel gain, given by [12–15]

$$n^* = \arg\max_{1\leq n\leq N} |h_n|^2, \tag{3}$$

where $h_n \sim \mathcal{CN}(0, \alpha)$ denotes the channel parameter of the wireless link from the user to the KG_n.

Then, the effective signal-to-noise ratio (SNR) of KG_{n^*} and eavesdropper can be written as [16, 17]

$$\begin{aligned} \mathrm{SNR}_{\mathrm{n}^*} &= \frac{P|h_{n^*}|^2}{\sigma^2}, \\ \mathrm{SNR}_{\mathrm{E}} &= \frac{P|g|^2}{\sigma^2}. \end{aligned} \tag{4}$$

Then, we can obtain the system transmission rate in the presence of one eavesdropper according to the Shannon Formula, which is [18, 19]

$$\begin{aligned} R &= [\log_2(1 + \mathrm{SNR}_{\mathrm{n}^*}) - \log_2(1 + \mathrm{SNR}_{\mathrm{E}})] \\ &= \log_2\left(\frac{\sigma^2 + P|h_{n^*}|^2}{\sigma^2 + P|g|^2}\right). \end{aligned} \tag{5}$$

3. Analysis of outage probability

3.1. One KG node

In this subsection, our goal is to measure the performance of the devised network in terms of outage probability, where the analytical expression for the network outage probability is derived. Since the eavesdropper can overhear the network and may cause physical-layer security problems, the outage probability is defined by [20]

$$P_{out} = \Pr\left\{\log_2\left(1 + \frac{P}{\sigma^2}|h|^2\right) - \log_2\left(1 + \frac{P}{\sigma^2}|g|^2\right) < R_{th}\right\}, \tag{6}$$

where R_{th} is the threshold. According to (6), the outage probability occurs when the value of $C_{sr} - C_{se} < R_{th}$, which means that the transmission fails to receive the signal from S to R. The equation (6) can be further written as [21–23]

$$\begin{aligned} P_{out} &= \Pr\left\{\log_2\left(\frac{\sigma^2 + P|h|^2}{\sigma^2 + P|g|^2}\right) < R_{th}\right\}, \\ &= \Pr\left\{|h|^2 < \frac{(A_0 - 1)\sigma^2 + P|g|^2}{P}\right\}, \\ &= \int_0^{+\infty}\int_0^{\frac{(A_0-1)\sigma^2+Px}{P}} \frac{\exp(-\frac{x}{\beta})\exp(-\frac{y}{\alpha})}{\alpha\beta}\mathrm{d}y\mathrm{d}x, \\ &= \frac{1}{\beta}\int_0^{+\infty}\exp(\frac{x}{\beta})\mathrm{d}x \\ &- \left\{\frac{1}{\beta}\int_0^{+\infty}\exp(\frac{(1 - A_0)\sigma^2}{P\alpha}) + \exp(\frac{-A_0 x}{\alpha})\right\}\mathrm{d}x, \\ &= 1 - \frac{\alpha}{\alpha + A_0\beta}\exp(\frac{(1 - A_0)\sigma^2}{P\alpha}), \end{aligned} \tag{7}$$

with $A_0 = 2^{R_{th}}$.

3.2. Multiple KG nodes

As to multiple KG nodes in the power system, we will also give the definition of the system outage probability and derive the associated closed-form expression of the outage probability under this network. In particular, the outage probability is that the system transmission rate is less than the stated threshold R_{th}, which can be denoted by [24, 25]

$$\begin{aligned} \mathrm{Pout} &= \Pr(R < R_{th}) \\ &= \Pr\left[\log_2\left(\frac{\sigma^2 + P|h_{n^*}|^2}{\sigma^2 + P|g|^2}\right) < R_{th}\right]. \end{aligned} \tag{8}$$

According to (8), we can know that the outage occurs when $R < R_{th}$.

Then, from (8), we can obtain [26–28]

$$\begin{aligned}\text{Pout} &= \Pr\left[|h_{n^*}|^2 < \frac{2^{R_{th}}(\sigma^2 + P|g|^2) - \sigma^2}{P}\right] \\ &= \int_0^{\frac{2^{R_{th}}(\sigma^2+P|g|^2)-\sigma^2}{P}} f_{|h_{n^*}|^2}(x)dx,\end{aligned} \tag{9}$$

where $f_{|h_{n^*}|^2}(x)$ is the probability density function (PDF) of the variable $|h_{n^*}|^2$. As $|h_n|^2 \sim \text{Exp}(\frac{1}{\alpha})$, we can obtain $f_{|h_n|^2}(x)$ as [29–31]

$$f_{|h_n|^2}(x) = \begin{cases} \frac{1}{\alpha}e^{-\frac{x}{\alpha}}, & x > 0, \\ 0, & x \leq 0. \end{cases} \tag{10}$$

Further, according to the order statistics and (10), the PDF of the $|h_{n^*}|^2$ can be obtain as [32–34]

$$f_{|h_{n^*}|^2}(x) = \begin{cases} \frac{N}{\alpha}e^{-\frac{x}{\alpha}}\left(1 - e^{-\frac{x}{\alpha}}\right)^{N-1}, & x > 0, \\ 0, & x \leq 0. \end{cases} \tag{11}$$

Consequently, according to (11), (9) can be re-written as

$$\begin{aligned}\text{Pout} &= \int_0^{\frac{2^{R_{th}}(\sigma^2+P|g|^2)-\sigma^2}{P}} \frac{N}{\alpha}e^{-\frac{x}{\alpha}}\left(1 - e^{-\frac{x}{\alpha}}\right)^{N-1} dx \\ &= \left[1 - e^{-\frac{2^{R_{th}}(\sigma^2+P|g|^2)-\sigma^2}{\alpha P}}\right]^N.\end{aligned} \tag{12}$$

In further, according to $|g|^2 \sim \text{Exp}(\frac{1}{\beta})$, we can obtain $f_{|g|^2}(x)$ as,

$$f_{|g|^2}(x) = \begin{cases} \frac{1}{\beta}e^{-\frac{x}{\beta}}, & x > 0, \\ 0, & x \leq 0. \end{cases} \tag{13}$$

Then, (12) can be re-written as

$$\begin{aligned}\text{Pout} &= \frac{1}{\beta}\int_0^{+\infty} e^{-\frac{x}{\beta}}\left[1 - e^{-\frac{2^{R_{th}}(\sigma^2+Px)-\sigma^2}{\alpha P}}\right]^N dx \\ &= \frac{1}{\beta}\int_0^{+\infty} e^{-\frac{x}{\beta}}\sum_{k=0}^{N}\binom{N}{k}(-1)^{N-k}e^{A(N-k)}e^{-B(N-k)x}dx \\ &= \frac{1}{\beta}\sum_{k=0}^{N-1}\binom{N}{k}(-1)^{N-k}e^{A(N-K)}\int_0^{+\infty} e^{-\frac{x}{\beta}}e^{-B(N-k)x}dx \\ &+ \frac{1}{\beta}\binom{N}{N}\int_0^{+\infty} e^{-\frac{x}{\beta}}dx,\end{aligned} \tag{14}$$

with

$$\begin{aligned}A &= \frac{(1 - 2^{R_{th}})\sigma^2}{\alpha P}, \\ B &= \frac{2^{R_{th}}}{\alpha}.\end{aligned} \tag{15}$$

Finally, according to (14), we can obtain the closed-form expression of outage probability in this network, which is

$$\text{Pout} = 1 + \sum_{k=0}^{N-1}\frac{\binom{N}{k}(-1)^{N-k}e^{A(N-k)}}{1 + \beta B(N-k)}. \tag{16}$$

In the next section, we will discuss the simulated result to verify the closed-form expression.

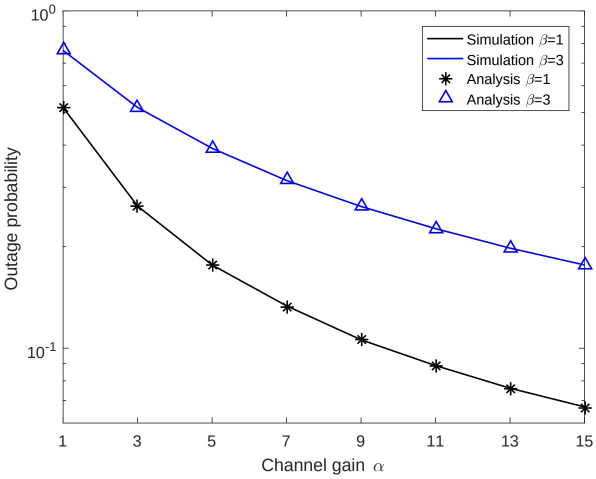

Figure 3. The effect of channel gain α on the power system transformer standard based on knowledge graph.

4. Analytical and Simulation Results

In this part, the simulated results are presented to verify the analytical results. In particular, the impacts of the network parameters such as α, β, and R_{th} on system secure performance are presented, and the corresponding results are shown in the following figure s. If not specified, the transmit power P is set to 1w, σ^2 is set to 0.1w, and R_{th} is set to 0.1.

Fig. 3 demonstrates the effect of channel gain α on the secure wireless network, where α goes from 1 to 15 and the value of β is 1 or 3. From fig. 3, we can find that the closed-form expression of the outage probability matches the simulated results very well, which verifies the validity of (7). Moreover, the value of outage probability decreases swiftly with the increasing value of α. This is because that a higher α can effectively improve the transmission rate, which further enhances the system secure transmission performance. For example, when $\alpha = 11$ with $\beta = 1$, the outage probability of the considered system is about 6%, which means the considered network has a better secure transmission environment under the eavesdropper.

Fig. 4 shows the effect of channel gain β on the secure wireless network, where β changes in the range of [1, 15] and the value of α is 1 or 5. As shown in Fig. 4, we can find an interesting circumstance that the value of outage probability increases rapidly when β becomes large. This is due to the fact that increasing β can

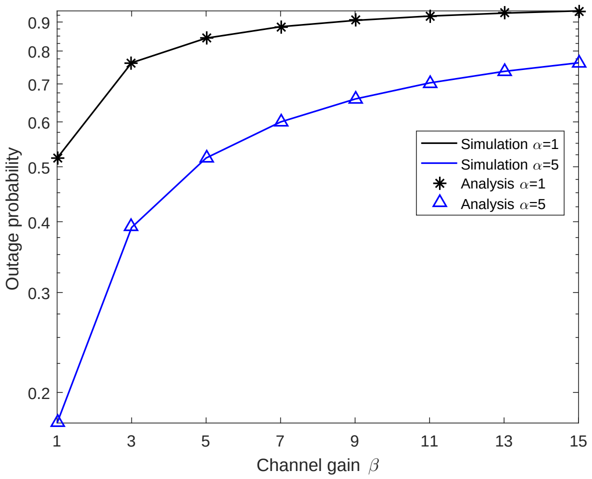

Figure 4. The effect of channel gain β on the power system transformer standard based on knowledge graph.

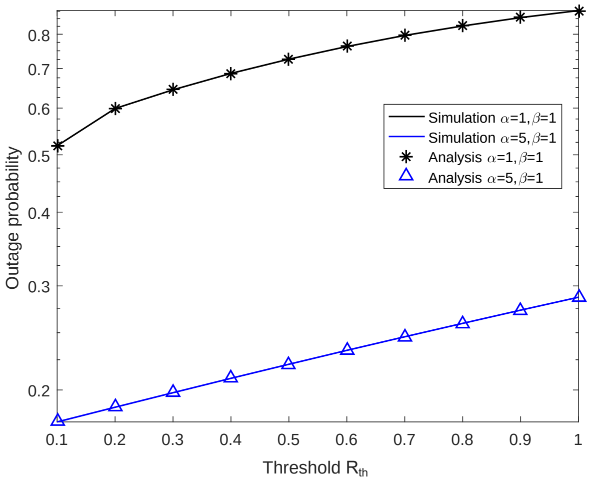

Figure 5. The impact of threshold R_{th} on the power system transformer standard based on knowledge graph.

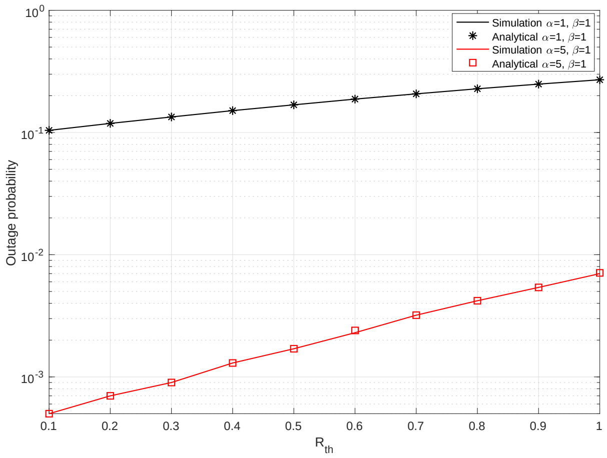

Figure 6. Outage probability of the power system transformer standard based on knowledge graph versus R_{th}.

enhance the transmit SNR from S to E, which improves the efficiency of eavesdropping, leading to difficulty for secure transmission between S to R and a higher outage probability for transmission. Moreover, the analytical results match the simulation very well, which verifies the derived closed-form expressions for the network average outage probability.

Fig. 5 represents the impact of threshold R_{th} on the considered networks, where $\beta = 1$, $\alpha = 1$ or $\alpha = 5$, and R_{th} fluctuates in $[0.1, 1.0]$. From Fig. 5, we can observe that for either $\alpha = 1$ or $\alpha = 5$ with various values of R_{th}, the closed-form outage probability fits well with the simulated one, which validates the correctness of the derived closed-form expression. In addition, the value of outage probability with $\alpha = 1$ is higher than that with $\alpha = 5$ no matter what the value of R_{th} is. This is due to the fact that increasing α can lead to a stronger link from the source S to R, improving the average channel capacity for transmission, and decreasing the outage probability event. For example, when $R_{th} = 0.5$, the outage probability with $\alpha = 5$ is 22%, while that with $\alpha = 1$ is 51%. The outage probability of the latter is about twice as high as the former, which demonstrates an interesting fact that a higher transmit SNR between S to R can improve the network transmission performance and enhance the physical-layer security.

In the following part, we show some simulations to verify the analytical result for the considered system with multiple KG nodes. If not specified, the environment setup of the simulations is set as follows. The number of KG node is set to $N = 10$, and the transmit power is set to $P = 10$ dB. The average channel gains are set to $\alpha = 1$ and $\beta = 1$, where the threshold is set to $R_{th} = 0.1$.

Fig. 6 shows the outage probability of the simulation and closed-form expression versus the threshold R_{th}, where the threshold is set to $R_{th} \in [0.1, 1]$, the value of α is 1 or 5, and the value of β is 1. From Fig. 6, we can observe that the system outage performance deteriorates with an increasing value of R_{th}, which indicates that the increasing value of R_{th} can possibility of outage event. Moreover, the analytical result is close to the simulated result, which shows the accuracy of the closed-form expression. In further, the system outage performance with $\alpha = 5$ is better than the the system outage performance with $\alpha = 1$, as the channel condition from the user to the selected KG node becomes better.

Fig. 7 illustrates the outage probability of the simulation and closed-form expression versus the average channel gain of the KG link α, where $\alpha \in [1, 10]$, the value of R_{th} is 1 or 5, and β is 1. We can observe from

Table 1 Data for Fig.6

R_{th}	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1
Sim:$\alpha = 1$	0.1041	0.1187	0.1340	0.1510	0.1684	0.1876	0.2071	0.2279	0.2488	0.2701
Ana:$\alpha = 1$	0.1041	0.1187	0.1340	0.1510	0.1684	0.1876	0.2071	0.2279	0.2488	0.2701
Sim:$\alpha = 5$	0.0005	0.0007	0.0009	0.0013	0.0017	0.0023	0.0032	0.0042	0.0054	0.0070
Ana:$\alpha = 5$	0.0005	0.0007	0.0009	0.0013	0.0017	0.0024	0.0032	0.0042	0.0054	0.0071

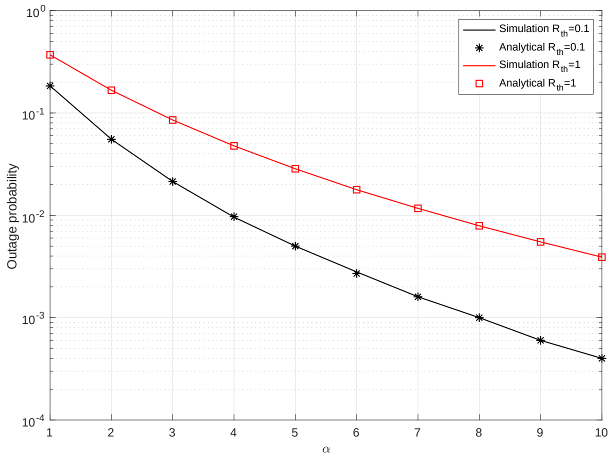

Figure 7. Outage probability of the power system transformer standard based on knowledge graph versus α.

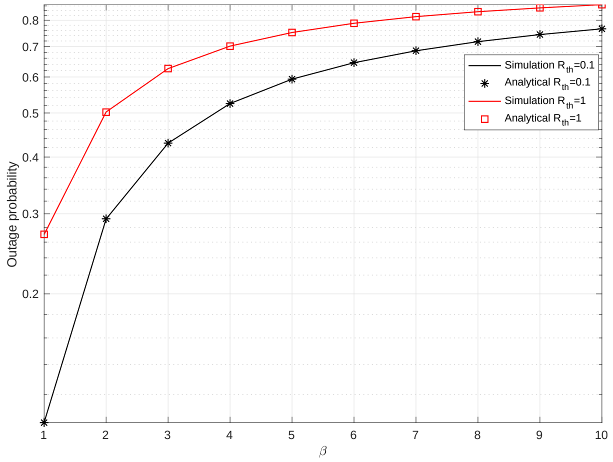

Figure 8. Outage probability of the network versus β.

Fig. 7 that the outage probability improves with a large value of α, due to the improved channel condition from the user to the selected KG node. In addition, as shown in Fig. 7, we can find that the outage probability with $R_{th} = 0.1$ is better than that with $R_{th} = 1$, which can lead to the same conclusion as from Fig. 6. Moreover, the analytical curve exactly matches the simulated result, which proves the correctness of the derived analytical expression.

Fig. 8 demonstrates the outage probability of the simulation and closed-form expression versus the average channel gain of the eavesdropping link β, where $\beta \in [1, 10]$, R_{th} is 1 or 5, and α is 1. We can find from Fig. 8 that as β increases, the system outage probability becomes worse, due to the improved channel conditions from the user to eavesdropper. Moreover, the analytical result is close to the simulated one, which demonstrates the validity of the derived closed-form expression.

5. Conclusions

The transformer could convert one kind of electric energy such as AC current and AC voltage into another kind of electric energy with the same frequency. KG could describe various entities and concepts in the real world and their relationships, and it could be considered as a semantic network for power system transformer. Hence, it was of vital importance to analyze and design the power system transformer standard based on the knowledge graph. To this end, we firstly examined the power system transformer with one KG node and one eavesdropper E, where the eavesdropper E could overhear the network from the source, which may cause physical-layer secure issue and an outage probability event. To deal with the issue, we analyzed and designed the system secure performance under the eavesdropper and defined the outage probability for system security, by providing analytical expression of outage probability. We further investigated the power system transformer with multiple KG nodes which could help strengthen the system security and reliability. For such a system, we analyzed and designed the system secure performance under the eavesdropper and defined the outage probability for system security, by providing analytical expression of outage probability. Finally, we gave some simulations to analyze the impact of secure transformer standard on the power system, and verified the accuracy of our proposed analytical expression for the the power system transformer standard based on the knowledge graph.

5.1. Data Availability Statement

The data of this work can be obtained through the email to the authors: Yuzhong Zhou (yuzhong_zhou@hotmail.com), Zhengping Lin (zhengping_lin@hotmail.com), Yuan La (yuanlacsg@hotmail.com), Junkai Huang

Table 1 Data for Fig.7

α	1	2	3	4	5	6	7	8	9	10
Sim:R_{th} = 0.1	0.1841	0.0554	0.0214	0.0096	0.0050	0.0028	0.0016	0.0010	0.0006	0.0004
Ana:R_{th} = 0.1	0.1839	0.0553	0.0214	0.0097	0.0050	0.0027	0.0016	0.0010	0.0006	0.0004
Sim:R_{th} = 1	0.3700	0.1668	0.0854	0.0477	0.0285	0.0178	0.0117	0.0079	0.0055	0.0039
Ana:R_{th} = 1	0.3700	0.1668	0.0854	0.0477	0.0285	0.0178	0.0117	0.0079	0.0055	0.0039

Table 1 Data for Fig.8

β	1	2	3	4	5	6	7	8	9	10
Sim:R_{th} = 0.1	0.1043	0.2923	0.4291	0.5245	0.5935	0.6450	0.6852	0.7176	0.7438	0.7658
Ana:R_{th} = 0.1	0.1042	0.2926	0.4292	0.5244	0.5934	0.6453	0.6856	0.7177	0.7440	0.7658
Sim:R_{th} = 1	0.2702	0.5025	0.6260	0.7016	0.7516	0.7876	0.8145	0.8351	0.8514	0.8656
Ana:R_{th} = 1	0.2704	0.5021	0.6262	0.7014	0.7517	0.7875	0.8144	0.8352	0.8519	0.8654

(junkaihuangcsg@hotmail.com) and Xin Wang (xinwangcsg@hotmail.com). As to this work, the authors would like to sincerely thank the following researchers for the meaningful discussions: Xiazhi Lai (xiazhilai@hotmail.com), Bowen Lu (bwlu@ieee.org), and Yinghao Guo (yinghaoguo@ieee.org).

5.2. Copyright

The Copyright was licensed to EAI.

References

[1] N. Dahlin and R. Jain, "Scheduling flexible nonpreemptive loads in smart-grid networks," *IEEE Trans. Control. Netw. Syst.*, vol. 9, no. 1, pp. 14–24, 2022.

[2] E. Z. Serper and A. Altin-Kayhan, "Coverage and connectivity based lifetime maximization with topology update for WSN in smart grid applications," *Comput. Networks*, vol. 209, p. 108940, 2022.

[3] Z. Alavikia and M. Shabro, "A comprehensive layered approach for implementing internet of things-enabled smart grid: A survey," *Digit. Commun. Networks*, vol. 8, no. 3, pp. 388–410, 2022.

[4] S. Mishra, "Blockchain-based security in smart grid network," *Int. J. Commun. Networks Distributed Syst.*, vol. 28, no. 4, pp. 365–388, 2022.

[5] H. Wang and Z. Huang, "Guest editorial: WWWJ special issue of the 21th international conference on web information systems engineering (WISE 2020)," *World Wide Web*, vol. 25, no. 1, pp. 305–308, 2022.

[6] H. Wang, J. Cao, and Y. Zhang, *Access Control Management in Cloud Environments*. Springer, 2020. [Online]. Available: https://doi.org/10.1007/978-3-030-31729-4

[7] H. Wang, Y. Wang, T. Taleb, and X. Jiang, "Editorial: Special issue on security and privacy in network computing," *World Wide Web*, vol. 23, no. 2, pp. 951–957, 2020.

[8] S. Tang, "Dilated convolution based CSI feedback compression for massive MIMO systems," *IEEE Trans. Vehic. Tech.*, vol. 71, no. 5, pp. 211–216, 2022.

[9] X. Hu, C. Zhong, Y. Zhu, X. Chen, and Z. Zhang, "Programmable metasurface-based multicast systems: Design and analysis," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1763–1776, 2020.

[10] S. Tang and L. Chen, "Computational intelligence and deep learning for next-generation edge-enabled industrial IoT," *IEEE Trans. Netw. Sci. Eng.*, vol. 9, no. 3, pp. 105–117, 2022.

[11] X. Hu, C. Zhong, Y. Zhang, X. Chen, and Z. Zhang, "Location information aided multiple intelligent reflecting surface systems," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7948–7962, 2020.

[12] X. Lai, "Outdated access point selection for mobile edge computing with cochannel interference," *IEEE Trans. Vehic. Tech.*, vol. 71, no. 7, pp. 7445–7455, 2022.

[13] D. Cai, P. Fan, Q. Zou, Y. Xu, Z. Ding, and Z. Liu, "Active device detection and performance analysis of massive non-orthogonal transmissions in cellular internet of things," *Science China information sciences*, vol. 5, no. 8, pp. 182 301:1–182 301:18, 2022.

[14] J. Lu and J. Xia, "Performance analysis for IRS-assisted MEC networks with unit selection," *Physical Communication*, vol. 2022, no. 8.

[15] K. He and Y. Deng, "Efficient memory-bounded optimal detection for GSM-MIMO systems," *IEEE Trans. Commun.*, vol. 70, no. 7, pp. 4359–4372, 2022.

[16] R. Zhao and M. Tang, "Profit maximization in cache-aided intelligent computing networks," *Physical Communication*, vol. PP, no. 99, pp. 1–10, 2022.

[17] L. Chen, "Physical-layer security on mobile edge computing for emerging cyber physical systems," *Computer Communications*, vol. PP, no. 99, pp. 1–12, 2022.

[18] S. Tang and X. Lei, “Collaborative cache-aided relaying networks: Performance evaluation and system optimization,” *IEEE Journal on Selected Areas in Communications*, vol. PP, no. 99, pp. 1–12, 2022.

[19] R. Zhao and M. Tang, “Impact of direct links on intelligent reflect surface-aided MEC networks,” *Physical Communication*, vol. PP, no. 99, pp. 1–10, 2022.

[20] L. Zhang and C. Gao, “Deep reinforcement learning based IRS-assisted mobile edge computing under physical-layer security,” *Physical Communication*, vol. PP, no. 99, pp. 1–10, 2022.

[21] L. Chen and X. Lei, “Relay-assisted federated edge learning:Performance analysis and system optimization,” *IEEE Transactions on Communications*, vol. PP, no. 99, pp. 1–12, 2022.

[22] J. Sun, X. Wang, Y. Fang, X. Tian, M. Zhu, J. Ou, and C. Fan, “Security performance analysis of relay networks based on-shadowed channels with rhis and cees,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[23] X. Deng, S. Zeng, L. Chang, Y. Wang, X. Wu, J. Liang, J. Ou, and C. Fan, “An ant colony optimization-based routing algorithm for load balancing in leo satellite networks,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[24] J. Lu and M. Tang, “Performance analysis for IRS-assisted MEC networks with unit selection,” *Physical Communication*, vol. PP, no. 99, pp. 1–10, 2022.

[25] Y. Wu and C. Gao, “Task offloading for vehicular edge computing with imperfect CSI: A deep reinforcement approach,” *Physical Communication*, vol. PP, no. 99, pp. 1–10, 2022.

[26] C. Wang, W. Yu, F. Zhu, J. Ou, C. Fan, J. Ou, and D. Fan, “Uav-aided multiuser mobile edge computing networks with energy harvesting,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[27] J. Chen, Y. Wang, J. Ou, C. Fan, X. Lu, C. Liao, X. Huang, and H. Zhang, “Albrl: Automatic load-balancing architecture based on reinforcement learning in software-defined networking,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[28] C. Ge, Y. Rao, J. Ou, C. Fan, J. Ou, and D. Fan, “Joint offloading design and bandwidth allocation for ris-aided multiuser mec networks,” *Physical Communication*, p. 101752, 2022.

[29] C. Yang, B. Song, Y. Ding, J. Ou, and C. Fan, “Efficient data integrity auditing supporting provable data update for secure cloud storage,” *Wireless Communications and Mobile Computing*, vol. 2022, 2022.

[30] J. Liu, Y. Zhang, J. Wang, T. Cui, L. Zhang, C. Li, K. Chen, S. Li, S. Feng, D. Xie *et al.*, “Outage probability analysis for uav-aided mobile edge computing networks,” *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 9, no. 31, pp. e4–e4, 2022.

[31] J. Liu, Y. Zhang, J. Wang, T. Cui, L. Zhang, C. Li, K. Chen, H. Huang, X. Zhou, W. Zhou *et al.*, “The intelligent bi-directional relaying communication for edge intelligence based industrial iot networks: Intelligent bi-directional relaying communication,” *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, vol. 9, no. 32, pp. e4–e4, 2022.

[32] Y. Tang and S. Lai, “Intelligent distributed data storage for wireless communications in b5g networks,” *EAI Endorsed Transactions on Mobile Communications and Applications*, vol. 2022, no. 8, pp. 121–128, 2022.

[33] ——, “Energy-efficient and high-spectrum-efficiency wireless transmission,” *EAI Endorsed Transactions on Mobile Communications and Applications*, vol. 2022, no. 8, pp. 129–135, 2022.

[34] J. Liu and W. Zhou, “Deep model training and deployment on scalable iot networks: A survery,” *EAI Endorsed Transactions on Scalable Information Systems*, vol. 2022, no. 2, pp. 29–35, 2022.