EAI Endorsed Transactions
on Scalable Information Systems
Research Article EAI.EU

Research on Intrusion Detection Technology of Computing Nodes in Digital Power Grid based on Artificial Intelligence

Xubin Lin[1,*], Situo Zhang[1], Feifei Hu[1], and Liu Wu[1]

[1]Power dispatching control center of China Southern Power Grid, Guangzhou, China.

Abstract

This paper aims to investigate an intrusion detection network for digital power grid networks, which consists of an edge server and two computational nodes that work collaboratively to detect any potential intrusion in the network. The primary objective of this study is to enhance the effectiveness of intrusion detection in the network. To achieve this objective, we first define the outage probability of the intrusion detection system under consideration. This is done to provide a measure of the probability that the system fails to detect an intrusion when it occurs. We then derive a closed-form expression for the outage probability to enable further analysis on the system behavior. Since the system resources, such as transmit power, are limited, we further design a transmit power allocation strategy to improve the system performance. This strategy seeks to optimize the allocation of transmit power across the different nodes of the intrusion detection network to maximize the likelihood of detecting intrusions while minimizing the resource usage. Finally, to evaluate the performance of the proposed system, we conduct simulations and provide results that demonstrate the accuracy of the closed-form expression and the effectiveness of the transmit power allocation strategy. These simulation results serve as evidence of the efficacy of the proposed approach in detecting intrusions in a resource-constrained network, especially for the digital power grid networks.

Received on 02 March 2023; accepted on 10 May 2023; published on 16 May 2023

Keywords: Intrusion detection, artificial intelligence, performance analysis.

doi:10.4108/eetsis.v10i3.3092

1. Introduction

In recent years, artificial intelligence (AI) has made remarkable progress in fields such as image and speech recognition, natural language processing, machine translation, autonomous driving, and intelligent gaming [1–3]. Meanwhile, with the development of new technologies such as deep learning and reinforcement learning, the scope and practicality of AI have been further expanded, which has not only driven the upgrading and transformation of traditional industries but also brought many new business opportunities and social benefits [4, 5].

The widespread application of the Internet of Things (IoT) has made wireless network security issues increasingly important [6, 7]. In wireless network, the channel is the fundamental medium for data transmission, and its stability and security are crucial for ensuring communication quality [8, 9]. However, due to various factors, the channel is often susceptible to interference and intrusion attacks. Channel intrusion detection, as an important part of wireless network security, aims to discover and identify malicious behavior in the network, in order to protect wireless networks from various threats and attacks. Channel intrusion detection indicates the process of detecting unauthorized access or activity within communication channels between computing systems, such as a wireless or wired network [10, 11]. In many cases, these channels represent critical pathways for transmitting sensitive data, making them attractive targets for attackers seeking

*Corresponding author. Email: xubinlin2023@hotmail.com, linxb2@csg.cn.

to compromise the confidentiality, integrity, and availability of an organization's information. As intrusion techniques continue to evolve and advance, traditional intrusion detection methods are no longer able to meet the practical security needs. Therefore, researchers have started exploring new intrusion detection methods based on artificial intelligence, including machine learning, deep learning, and other emerging technologies. In this field, the authors in [12] proposed a novel approach for detecting insider threats in computer systems, where graph-based intelligence techniques were used to analyze the interactions between users and computer resources. In addition, a knowledge-driven approach was proposed for discovering software vulnerabilities and predicting co-exploitation behaviors, in which a hybrid approach combining data-driven techniques with expert knowledge was used to identify potential vulnerabilities and their co-exploitation behaviors [13]. In further, an integrated framework was proposed for predicting the time-to-exploit vulnerabilities in computer systems, where a dynamic imbalanced learning approach was devised to exploit the evolving nature of the system and the imbalanced distribution of vulnerabilities [14]. These methods can detect and prevent intrusion attacks by analyzing network traffic, identifying abnormal behavior and pattern recognition, and other techniques.

This paper focuses on the design and evaluation of an intrusion detection system for digital power grid networks. The system consists of an edge server and two computational nodes that work collaboratively to detect potential intrusions in the network. The primary objective of the study is to enhance the effectiveness of intrusion detection in the network while considering resource constraints, such as limited transmit power. To achieve this objective, the paper first defines the outage probability of the intrusion detection system, which provides a measure of the probability that the system fails to detect an intrusion when it occurs. The paper then derives a closed-form expression for the outage probability, enabling further analysis of the system behavior. To improve the system's performance, the paper designs a transmit power allocation strategy to optimize the allocation of transmit power across the different nodes of the intrusion detection network. This strategy aims to maximize the likelihood of detecting intrusions while minimizing the resource usage. Finally, the paper conducts simulations to evaluate the proposed system's performance and provides evidence of the efficacy of the closed-form expression and the transmit power allocation strategy in detecting intrusions in a resource-constrained network. The simulation results demonstrate the accuracy of the proposed approach and highlight its effectiveness, particularly for digital power grid networks.

The rest parts of this paper are summarized as follows. Sec. 2 describes the system model of intrusion detection for digital power grid networks, Sec. 3 defines the outage probability in this considered network, discusses the system optimization problem and designs the system resource allocation strategy. Sec. 4 provides some simulation results to verify the correctness of the closed-form expression and the effectiveness of our proposed transmit power allocation strategy. Sec. 5 gives the conclusion of this paper.

2. System model

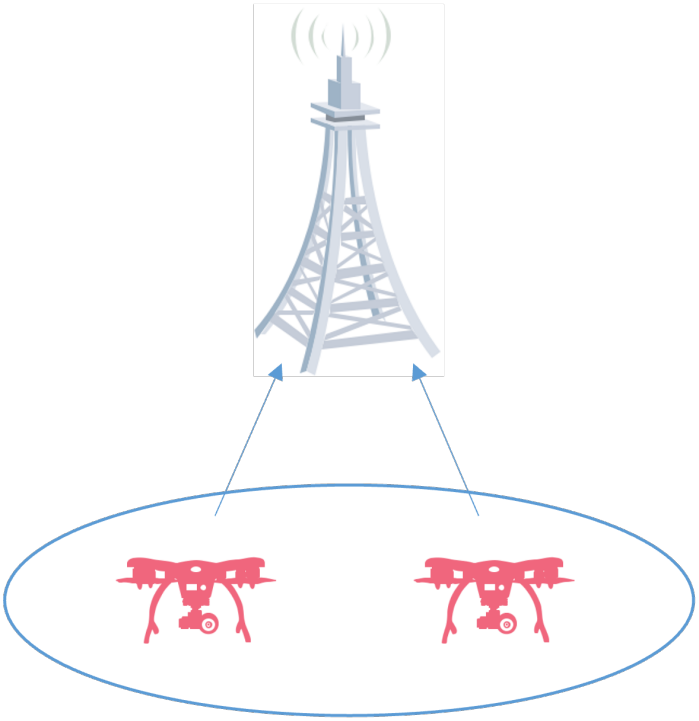

Figure 1. System model of intrusion detection with two computational nodes and an edge server for digital power grid networks.

Fig. 1 shows the system model of the intrusion detection with two computational nodes and an edge server for digital power grid networks, where there are two computational nodes $\{N_1, N_2\}$ and one edge server. Specifically, we assume that each computational node is equipped with one antenna for communicating with the edge server through an wireless link. Without loss of generality, the edge server conducts the intrusion detection of the computational nodes based on the signal-to ratio (SNR). In this network, the instantaneous SNR received by the edge server from the computational node N_1 is given by [15],

$$\mathrm{SNR}_1 = \frac{P_1|h_1|^2}{\sigma^2}, \tag{1}$$

where $h_1 \sim \mathcal{CN}(0, \beta_1)$ denotes the channel parameter of the wireless link from the computational node N_1 to the edge server. Moreover, P_1 is the transmit power at the computational node N_1, and σ^2 denotes the variance of the additional white Gaussian noise (AWGN) at the edge server.

In addition, the instantaneous SNR received by the edge server from the computational node N_2 is written as,

$$\mathrm{SNR}_2 = \frac{P_2|h_2|^2}{\sigma^2}, \tag{2}$$

where $h_2 \sim \mathcal{CN}(0, \beta_2)$ is the channel gain of the wireless link from the computational node N_2 to the edge server, and P_2 denotes the transmit power at the computational node N_2. Particularly, P_1 and P_2 should satisfy the following constraint [16, 17],

$$P_1 + P_2 = P, \tag{3}$$

where P denotes the total transmit power of the computational nodes.

Without loss of generality, we assume that the edge server can successfully complete the intrusion detection if and only if it can simultaneously satisfy the following two constraints,

$$\mathrm{SNR}_1 \geq \gamma_1, \tag{4}$$

$$\mathrm{SNR}_2 \geq \gamma_2, \tag{5}$$

where γ_1 and γ_2 denote the SNR threshold received by the edge server from the computational nodes N_1 and N_2, respectively. When $\mathrm{SNR}_1 \geq \gamma_1$ and $\mathrm{SNR}_2 \geq \gamma_2$ both hold, the edge server will successfully detect the intrusion.

3. Problem formulation and optimization

In this section, we elaborate the system optimization problem of the considered digital power grid networks. Specifically, we firstly define the system outage probability, which is equal to the probability of failing the intrusion detection, and then derive the corresponding closed-form expression. In further, we aim to improve the system performance by minimizing the system outage probability, through optimizing the transmit power of the computational nodes N_1 and N_2.

From (4) and (5), the outage probability is defined as the probability that SNR_1 and SNR_2 are less than the associated SNR thresholds γ_1 and γ_2 respectively,

$$P_{out} = \Pr(\mathrm{SNR}_1 < \gamma_1 \parallel \mathrm{SNR}_2 < \gamma_2), \tag{6}$$

where $\mathrm{SNR}_1 < \gamma_1$ and $\mathrm{SNR}_2 < \gamma_2$ mean the outage occurs at N_1 and N_2, respectively.

From (6), we can further derive as [18, 19],

$$P_{out} = \Pr\left(\frac{P_1|h_1|^2}{\sigma^2} < \gamma_1 \parallel \frac{P_2|h_2|^2}{\sigma^2} < \gamma_2\right), \tag{7}$$

According to (3) and (7), we can obtain,

$$P_{out} = \Pr\left(\frac{P_1|h_1|^2}{\sigma^2} < \gamma_1 \parallel \frac{(P-P_1)|h_2|^2}{\sigma^2} < \gamma_2\right), \tag{8}$$

$$= \Pr\left(\frac{P_1|h_1|^2}{\sigma^2} < \gamma_1\right)\Pr\left(\frac{(P-P_1)|h_2|^2}{\sigma^2} < \gamma_2\right), \tag{9}$$

$$= \Pr\left(|h_1|^2 < \frac{\gamma_1\sigma^2}{P_1}\right)\Pr\left(|h_2|^2 < \frac{\gamma_2\sigma^2}{(P-P_1)}\right), \tag{10}$$

$$= \int_0^{\frac{\gamma_1\sigma^2}{P_1}} f_{|h_1|^2}(x)dx \int_0^{\frac{\gamma_2\sigma^2}{P-P_1}} f_{|h_2|^2}(y)dy, \tag{11}$$

where $f_{|h_1|^2}(x)$ and $f_{|h_2|^2}(y)$ denote the probability density functions (PDF) of $|h_1|^2$ and $|h_2|^2$, respectively. According to the $|h_1|^2 \sim \mathrm{Exp}(\frac{1}{\beta_1})$, we can first get $f_{|h_1|^2}$ as,

$$f_{|h_1|^2}(x) = \begin{cases} \frac{1}{\beta_1}e^{-\frac{x}{\beta_1}}, & x > 0, \\ 0, & x \leq 0. \end{cases} \tag{12}$$

Moreover, according to the $|h_2|^2 \sim \mathrm{Exp}(\frac{1}{\beta_2})$, we can also obtain $f(|h_2|^2)(y)$ as,

$$f_{|h_2|^2}(y) = \begin{cases} \frac{1}{\beta_2}e^{-\frac{y}{\beta_2}}, & y > 0, \\ 0, & y \leq 0. \end{cases} \tag{13}$$

From (11), (12) and (13), we can further derive P_{out} as,

$$P_{out} = \int_0^{\frac{\gamma_1\sigma^2}{P_1}} \frac{1}{\beta_1}e^{-\frac{x}{\beta_1}}dx \int_0^{\frac{\gamma_2\sigma^2}{P-P_1}} \frac{1}{\beta_2}e^{-\frac{y}{\beta_2}}dy, \tag{14}$$

$$= \left(1 - e^{-\frac{\gamma_1\sigma^2}{\beta_1 P_1}}\right)\left(1 - e^{-\frac{\gamma_2\sigma^2}{\beta_2(P-P_1)}}\right). \tag{15}$$

In this way, we can obtain the closed-form expression of the system outage probability in this considered network. In further, we can improve the system performance by minimizing the outage probability, through optimizing the transmit power of the computational nodes N_1 and N_2, given by,

$$\min_{\{P_1,P_2\}} \quad \left(1 - e^{-\frac{\gamma_1\sigma^2}{\beta_1 P_1}}\right)\left(1 - e^{-\frac{\gamma_2\sigma^2}{\beta_2(P-P_1)}}\right) \tag{16a}$$

$$\text{s.t.} \quad C_1 : 0 \leq P_1 \leq P. \tag{16b}$$

Specifically, constraint C_1 indicates that the transmit power of the computational node N_1 should not exceed the total system transmit power. In the following, we will describe a transmit power allocation schemes to solve the optimization problem.

In this section, we propose two transmit power allocation schemes for the digital power grid networks to improve the system performance, by minimizing the

Table 1 Data for Fig. 2

P	5	10	15	20	25
Pro:γ_1=0.1 ($\times e^{-06}$)	15.940	3.992	1.775	0.999	0.640
Bf:γ_1=0.1 ($\times e^{-06}$)	15.940	3.992	1.775	0.999	0.640
Sim:γ_1=0.1 ($\times e^{-06}$)	16.020	4.052	1.801	1.108	0.700
Pro:γ_1=0.2 ($\times e^{-06}$)	31.800	7.976	3.548	1.997	1.278
Bf:γ_1=0.2 ($\times e^{-06}$)	31.800	7.976	3.548	1.997	1.278
Sim:γ_1=0.2 ($\times e^{-06}$)	31.800	7.968	3.542	1.997	1.269
Pro:γ_1=0.3 ($\times e^{-06}$)	47.620	11.950	5.319	2.994	1.917
Bf:γ_1=0.3 ($\times e^{-06}$)	47.620	11.950	5.319	2.994	1.917
Sim:γ_1=0.3 ($\times e^{-06}$)	47.120	11.910	5.310	2.992	1.917

system outage probability. The details of two proposed allocation scheme are elaborated in the follow.

Considering the fairness of each computational node, we can uniformly allocate the transmit power to the computational nodes, which can be described as,

$$P_1 = \frac{P}{2}, \tag{17}$$

$$P_2 = \frac{P}{2}. \tag{18}$$

Besides the uniform power allocation in the above, we can also use the efficient dichotomy method to perform the power allocation between the two users. Specifically, the dichotomy method, also known as the bisection method, is a numerical algorithm used to find the roots of a continuous function. The method involves repeatedly bisecting an interval and then selecting a subinterval in which a root must lie, based on the sign of the function at the endpoints of the interval. The process is repeated until a root is found with a desired level of accuracy. The dichotomy method is a simple and robust algorithm that can be applied to a wide range of functions. It does not require knowledge of the derivative of the function, making it useful for functions that are difficult or expensive to differentiate. However, the method is relatively slow compared to some other root-finding algorithms, especially when the function has multiple roots or a steep slope near the root. In addition to finding roots, the dichotomy method can also be used to find the maximum or minimum value of a unimodal function on a closed interval. This is done by replacing the sign of the function with its derivative in the algorithm, and modifying the subinterval selection criteria accordingly.

4. Simulation

In this section, we present some experiments for the digital power grid networks, to demonstrate the effectiveness of our proposed resource allocation schemes. If not specified, the total transmit power is set to 15W.

Fig. 2 and Table 1 depict the impact of the total transmit power on the system outage probability of digital power grid networks, where $\beta_1 = 0.1$, $\beta_2 = 0.2$, $\gamma_1 = 0.1$, $\gamma_2 = 0.2$, and the total transmit power varies

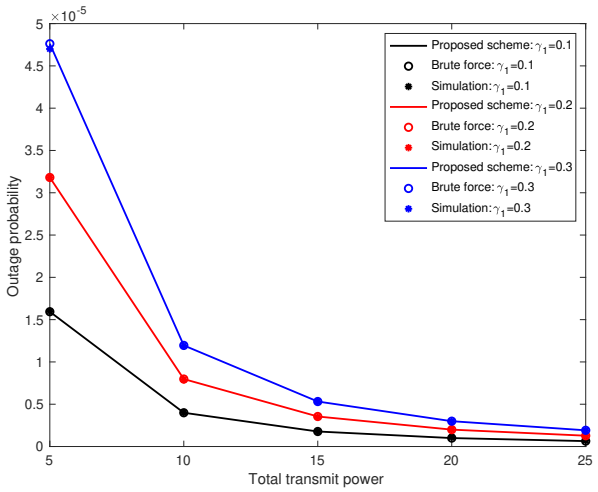

Figure 2. Outage probability of the considered system versus the total transmit power.

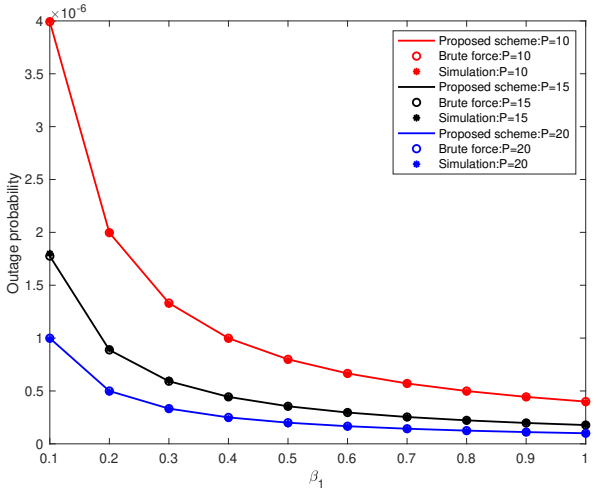

Figure 3. Outage probability of the considered system versus β_1.

from 5W to 25W. For comparison, we provide the result of "Brute force" scheme, which can find the optimal solution by iterating over all feasible solutions. As observed from this figure, we can see that the outage probability decreases as the total transmit power increases. This is because that a larger transmit power can provide a larger SNR. Moreover, the analytical results of our proposed scheme match well with the simulated ones, which demonstrates the effectiveness of the analytical expression. In further, our proposed scheme can achieve the same performance as the "Brute force", which verifies that validity of our proposed scheme.

Figs. 3 -4 and Table 2-3 show the impact of the rate parameters of exponential distribution on the outage

Table 2 Data for Fig. 3

β_1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
Pro:P=10 ($\times e^{-06}$)	3.992	1.997	1.332	0.999	0.799	0.666	0.571	0.499	0.444	0.400
Bf:P=10 ($\times e^{-06}$)	3.992	1.997	1.332	0.999	0.799	0.666	0.571	0.499	0.444	0.400
Sim:P=10 ($\times e^{-06}$)	4.052	2.001	1.328	0.999	0.798	0.665	0.569	0.498	0.444	0.400
Pro:P=15 ($\times e^{-06}$)	1.775	0.888	0.592	0.444	0.355	0.296	0.254	0.222	0.197	0.178
Bf:P=15 ($\times e^{-06}$)	1.775	0.888	0.592	0.444	0.355	0.296	0.254	0.222	0.197	0.178
Sim:P=15 ($\times e^{-06}$)	1.801	0.900	0.601	0.441	0.355	0.300	0.254	0.222	0.202	0.180
Pro:P=20 ($\times e^{-06}$)	0.999	0.500	0.333	0.250	0.200	0.167	0.143	0.125	0.111	0.100
Bf:P=20 ($\times e^{-06}$)	0.999	0.500	0.333	0.250	0.200	0.167	0.143	0.125	0.111	0.100
Sim:P=20 ($\times e^{-06}$)	1.108	0.498	0.332	0.248	0.199	0.167	0.140	0.122	0.109	0.099

Table 3 Data for Fig. 4

β_2	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
Pro:P=10 ($\times e^{-06}$)	7.976	3.992	2.662	1.997	1.598	1.332	1.141	0.999	0.888	0.799
Bf:P=10 ($\times e^{-06}$)	7.976	3.992	2.662	1.997	1.598	1.332	1.141	0.999	0.888	0.799
Sim:P=10 ($\times e^{-06}$)	8.001	4.052	2.641	1.980	1.586	1.315	1.111	0.990	0.881	0.796
Pro:P=15 ($\times e^{-06}$)	3.548	1.775	1.184	0.888	0.710	0.592	0.508	0.444	0.395	0.355
Bf:P=15 ($\times e^{-06}$)	3.548	1.775	1.184	0.888	0.710	0.592	0.508	0.444	0.395	0.355
Sim:P=15 ($\times e^{-06}$)	3.520	1.801	1.200	0.890	0.710	0.603	0.510	0.441	0.401	0.351
Pro:P=20 ($\times e^{-06}$)	1.997	0.999	0.666	0.500	0.400	0.333	0.286	0.250	0.222	0.200
Bf:P=20 ($\times e^{-06}$)	1.997	0.999	0.666	0.500	0.400	0.333	0.286	0.250	0.222	0.200
Sim:P=20 ($\times e^{-06}$)	1.983	1.108	0.661	0.497	0.390	0.333	0.284	0.249	0.222	0.198

Table 4 Data for Fig. 5

γ_1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
Pro:P=10 ($\times e^{-06}$)	3.992	7.976	11.952	15.920	19.880	23.833	27.777	31.714	35.642	39.563
Bf:P=10 ($\times e^{-06}$)	3.992	7.976	11.952	15.920	19.880	23.833	27.777	31.714	35.642	39.563
Sim:P=10 ($\times e^{-06}$)	4.052	7.973	11.715	16.000	19.797	23.699	27.681	31.714	36.001	39.610
Pro:P=15 ($\times e^{-06}$)	1.775	3.548	5.319	7.087	8.853	10.627	12.378	14.137	15.894	17.648
Bf:P=15 ($\times e^{-06}$)	1.775	3.548	5.319	7.087	8.853	10.627	12.378	14.137	15.894	17.648
Sim:P=15 ($\times e^{-06}$)	1.801	3.511	5.232	7.190	8.900	10.627	12.360	14.092	16.001	17.499
Pro:P=20 ($\times e^{-06}$)	0.999	1.997	2.994	3.990	4.985	5.979	6.972	7.964	8.955	9.945
Bf:P=20 ($\times e^{-06}$)	0.999	1.997	2.994	3.990	4.985	5.979	6.972	7.964	8.955	9.945
Sim:P=20 ($\times e^{-06}$)	1.108	1.979	2.976	3.970	4.969	6.005	6.960	8.000	8.959	9.945

Table 5 Data for Fig. 6

γ_2	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	1.0
Pro:P=10 ($\times e^{-06}$)	1.997	3.992	5.985	7.976	9.965	11.952	13.937	15.920	17.901	19.880
Bf:P=10 ($\times e^{-06}$)	1.997	3.992	5.985	7.976	9.965	11.952	13.937	15.920	17.901	19.880
Sim:P=10 ($\times e^{-06}$)	1.971	4.052	5.973	7.981	9.952	12.000	13.937	15.918	17.901	19.880
Pro:P=15 ($\times e^{-06}$)	0.888	1.775	2.662	3.548	4.434	5.319	6.204	7.087	7.971	8.853
Bf:P=15 ($\times e^{-06}$)	0.888	1.775	2.662	3.548	4.434	5.319	6.204	7.087	7.971	8.853
Sim:P=15 ($\times e^{-06}$)	0.900	1.801	2.658	3.542	4.416	5.300	6.210	7.104	8.000	8.902
Pro:P=20 ($\times e^{-06}$)	0.500	0.999	1.498	1.997	2.496	2.994	3.492	3.990	4.488	4.985
Bf:P=20 ($\times e^{-06}$)	0.500	0.999	1.498	1.997	2.496	2.994	3.492	3.990	4.488	4.985
Sim:P=20 ($\times e^{-06}$)	0.499	1.108	1.500	1.979	2.490	2.970	3.492	3.990	4.492	4.967

probability of digital power grid networks, where $\gamma_1 = 0.1$, $\gamma_2 = 0.2$, $P = 15$W. Moreover, we set $\beta_1 = 0.1$ in Fig. 3 and $\beta_2 = 0.2$ in Fig. 4. In particular, Fig. 3 and Fig. 4 correspond to $|h_1|^2$ and $|h_2|^2$, respectively. As shown in Figs. 3 -4 and Table 2-3, we can observe that the outage probability decreases with the increasing value of β_1 and β_2, since the channel quality is improved when β_1 and β_2 are larger. In addition, the analytical results of our proposed scheme fit well with the simulated ones, indicating that correctness of our analytical expression can be reliable. We can also see that the performance of our proposed scheme is equal to that of the "Brute force", which proves the effectiveness of our proposed scheme.

Figs. 5-6 and Table 4-5 present the impact of SNR thresholds on the outage probability of digital power grid networks, where $\beta_1 = 0.1$, $\beta_2 = 0.2$, $P = 15$W. Moreover, we set $\gamma_1 = 0.1$ in Fig. 5 and $\gamma_2 = 0.2$ in Fig. 6. Particularly, Fig. 5 and Fig. 6 correspond to the computational nodes N_1 and N_2, respectively. From Figs. 5-6 and Table 4-5, we can find that the outage probability increases with a larger γ_1 and γ_2, as the larger SNR threshold makes the intrusion detection more difficult. Besides, the analytical results of our proposed scheme match well with the simulated ones, which verifies the correctness of out analytical expression. We can also see that the performance of our proposed scheme can achieve the same performance as the "Brute force", which further demonstrates the effectiveness of our proposed scheme.

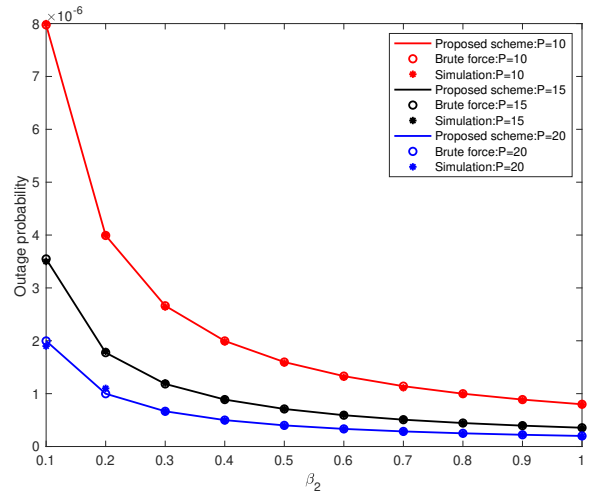

Figure 4. Outage probability of the considered system versus β_2.

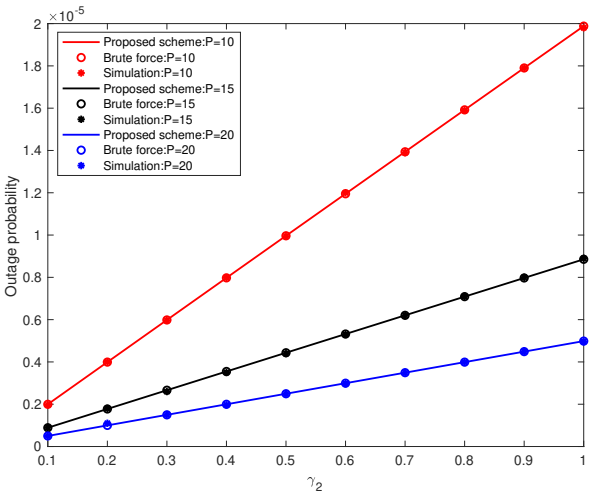

Figure 6. Outage probability of the considered system versus γ_2.

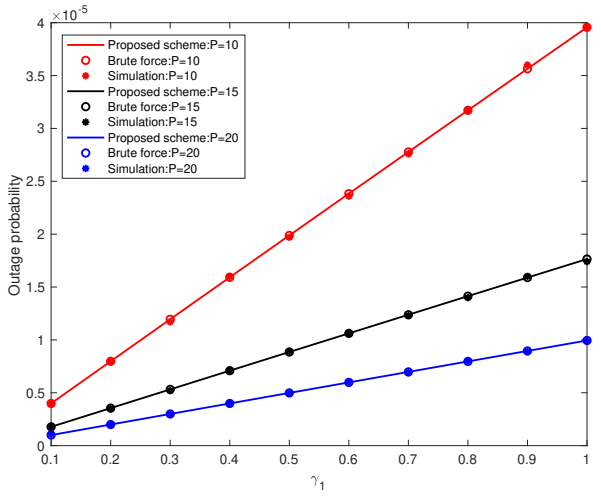

Figure 5. Outage probability of the considered system versus γ_1.

5. Conclusion

In this paper, we investigated the intrusion detection system with a edge server and two computational nodes for the digital power grid networks. Moreover, the edge server and computational nodes cooperatively detect the intrusion. To improve the effectiveness of the intrusion detection, we first defined the outage probability of the considered system, and then derived the closed-form expression. As the total transmit power is limited, we further optimized the transmit power allocation strategy to improve the system performance. Finally, some simulation results were provided to demonstrate the correctness of the closed-form expression and the effectiveness of our proposed transmit power allocation strategy.

5.1. Acknowledgements

This work was supported by the National Key RD Program of China(2020YFB0906003).

5.2. Copyright

References

[1] H. Yao, X. Li, and X. Yang, "Physics-aware learning-based vehicle trajectory prediction of congested traffic in a connected vehicle environment," *IEEE Trans. Veh. Technol.*, vol. 72, no. 1, pp. 102–112, 2023.

[2] J. Lin, G. Wang, S. Atapattu, R. He, G. Yang, and C. Tellambura, "Transmissive metasurfaces assisted wireless communications on railways: Channel strength evaluation and performance analysis," *IEEE Trans. Commun.*, 2023.

[3] L. F. Abanto-Leon, A. Asadi, A. Garcia-Saavedra, G. H. Sim, and M. Hollick, "Radiorchestra: Proactive management of millimeter-wave self-backhauled small cells via joint optimization of beamforming, user association, rate selection, and admission control," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 1, pp. 153–173, 2023.

[4] Y. Sun, D. Wu, X. S. Fang, and J. Ren, "On-glass grid structure and its application in highly-transparent antenna for internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 72, no. 1, pp. 93–101, 2023.

[5] Z. Na, B. Li, X. Liu, J. Wan, M. Zhang, Y. Liu, and B. Mao, "Uav-based wide-area internet of things: An integrated deployment architecture," *IEEE Netw.*, vol. 35, no. 5, pp. 122–128, 2021.

[6] W. Wu, F. Yang, F. Zhou, Q. Wu, and R. Q. Hu, "Intelligent resource allocation for IRS-enhanced OFDM communication systems: A hybrid deep reinforcement learning approach," *IEEE Trans. Wirel. Commun.*, vol. PP, no. 99, pp. 1–10, 2023.

[7] M. Sun, W. Liu, J. Liu, and C. Hao, "Complex parameter rao, wald, gradient, and durbin tests for multichannel signal detection," *IEEE Trans. Signal Process.*, vol. 70, pp. 117–131, 2022.

[8] W. Zhou, C. Li, and M. Hua, "Worst-case robust MIMO transmission based on subgradient projection," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 239–243, 2021.

[9] Z. Xuan and K. Narayanan, "Low-delay analog joint source-channel coding with deep learning," *IEEE Trans. Commun.*, vol. 71, no. 1, pp. 40–51, 2023.

[10] J. Shao, Y. Mao, and J. Zhang, "Task-oriented communication for multidevice cooperative edge inference," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 1, pp. 73–87, 2023.

[11] F. Liu, Y. Liu, A. Li, C. Masouros, and Y. C. Eldar, "Cramér-rao bound optimization for joint radar-communication beamforming," *IEEE Trans. Signal Process.*, vol. 70, pp. 240–253, 2022.

[12] W. Hong, J. Yin, M. You, H. Wang, J. Cao, J. Li, and M. Liu, "Graph intelligence enhanced bi-channel insider threat detection," in *Network and System Security: 16th International Conference, NSS 2022, Denarau Island, Fiji, December 9–12, 2022, Proceedings*. Springer, 2022, pp. 86–102.

[13] J. Yin, M. Tang, J. Cao, M. You, H. Wang, and M. Alazab, "Knowledge-driven cybersecurity intelligence: software vulnerability co-exploitation behaviour discovery," *IEEE Transactions on Industrial Informatics*, 2022.

[14] J. Yin, M. Tang, J. Cao, H. Wang, M. You, and Y. Lin, "Vulnerability exploitation time prediction: an integrated framework for dynamic imbalanced learning," *World Wide Web*, pp. 1–23, 2022.

[15] Z. Song, J. An, G. Pan, S. Wang, H. Zhang, Y. Chen, and M. Alouini, "Cooperative satellite-aerial-terrestrial systems: A stochastic geometry model," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 1, pp. 220–236, 2023.

[16] D. Orlando, S. Bartoletti, I. Palamà, G. Bianchi, and N. Blefari-Melazzi, "Innovative attack detection solutions for wireless networks with application to location security," *IEEE Trans. Wirel. Commun.*, vol. 22, no. 1, pp. 205–219, 2023.

[17] M. E. Gonzalez, J. F. Silva, M. Videla, and M. E. Orchard, "Data-driven representations for testing independence: Modeling, analysis and connection with mutual information estimation," *IEEE Trans. Signal Process.*, vol. 70, pp. 158–173, 2022.

[18] J. Ren, X. Lei, Z. Peng, X. Tang, and O. A. Dobre, "Ris-assisted cooperative NOMA with SWIPT," *IEEE Wireless Communications Letters*, 2023.

[19] W. Xu, Z. Yang, D. W. K. Ng, M. Levorato, Y. C. Eldar, and M. Debbah, "Edge learning for B5G networks with distributed signal processing: Semantic communication, edge computing, and wireless sensing," *IEEE J. Sel. Top. Signal Process.*, vol. 17, no. 1, pp. 9–39, 2023.