Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 4, pp. 2656–2663, DOI 10.12694/scpe.v25i4.2971

CONSTRUCTION AND ANALYSIS OF INTELLIGENT ANALYSIS AND DISPOSAL MODEL FOR INTERNET SECURITY EVENTS IN POWER SYSTEM

ZHENHONG ZHANG *, JIAN HU †, FEILU HANG ‡, AND LINJIANG XIE §

Abstract. The reliability of nodes is rugged to determine, and the global accuracy is low in identifying secure access nodes of ubiquitous power network gateways. Therefore, this project intends to establish a universal power grid gateway security access node identification model. Sensor technology collects secure access nodes of IoT gateways and evaluates their reliability. It is integrated with the security level of the network to form a virtual security domain. Then, the access node is searched and controlled twice. The access node identification of the universal power IoT gateway is realized according to the reliability calculation. Simulation results show that under the same parameter conditions, when the node size increases and the number of malicious nodes increases, the proposed method can obtain higher accuracy of secure access to nodes. This proves the advantages of the proposed method.

Key words: Power Internet of Things; Internet security incidents; Intelligent analysis; Internet of Things gateway; Secure access node

1. Introduction. With the continuous development of the intelligent grid, higher requirements are put forward for the security, aggression and vulnerability of power communication networks. The electric power communication network is a crucial link in the power grid, divided into different levels according to different business categories. In the whole system, the node is a very critical link. The failure of the node may cause particular interference to many services and even lead to the paralysis of some services. In the power communication network environment, node failure may interrupt higher-level power communication network services or lead to transmission delay problems. This has a significant impact on the operation of the entire power grid. Therefore, to reduce the vulnerability and danger in the network, it must be effectively identified and protected.

Many researchers at home and abroad are studying the problems related to the power grid. Literature [1] proposes a 5G-based distributed test system for power communication networks. The performance parameters of the network, transport, and application layers are measured. The probe detects each parameter to evaluate the whole power grid's operation comprehensively. However, this method does not measure the importance of critical nodes in the power network. According to the degree of shortest route selection, literature [2] gives the routing scheme of the power communication network. Then, they propose a link bandwidth utilization prediction method based on convolutional networks on graphs. The triangle module operator calculates the optimal path selection degree. Then, perform link optimization configuration. Document [3] A routing optimization method for power communication networks using PageRank. The research includes establishing the topology of the communication network and obtaining its characteristics. The PageRank algorithm is used to identify the critical nodes in the communication network. Set communication paths and metrics to maximize the use of information resources. Reference [3] studies the power system alarm signal fusion algorithm based on noise suppression. The alarm model of each node's message-receiving status is constructed based on each node's

*Network Security Management Center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000 (zhangzh202304@126.com)
†Network Security Management Center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000
‡Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000
§Information security operation and maintenance center of Information Center of Yunnan Power Grid Co., LTD., Kunming, Yunnan, China, 650000

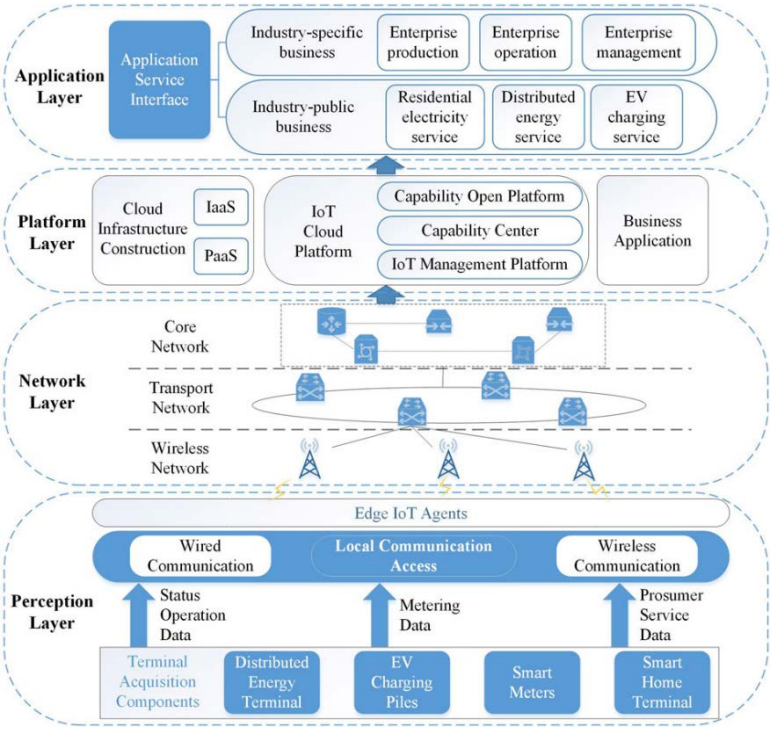

Fig. 2.1: *Data sensing mode in a ubiquitous electrical IoT.*

operation status and information-receiving status in the power network communication network. Literature [4] puts forward a cross-domain fusion framework applicable to power systems under the framework of IMS. After connecting different cross-domain websites, the access layer transforms them through the control protocol of the gateway to achieve the purpose of cross-domain IP access. The power communication service passes through the transport layer's Go interface, NGN packet core network and media gateway.

Transfer the multimedia Explorer to the control function of the media gateway in the session layer. The above research only discusses the influence of the shortest circuit and the optimal route composed of network nodes on the network topology. In the power system, if the critical node only carries many standard services but does not undertake the main business, the importance of this node is not high. Even if this node fails, it will not cause too much shock to the entire grid. Therefore, it is necessary to evaluate each node's importance in the power network comprehensively. This project intends to build a multi-level node importance identification method that includes the transport, physical topology, and service layers to improve the identification accuracy of critical nodes in the power grid.

2. Identify secure access nodes that are ubiquitous on the network gateway. In the universal power Internet of Things, all kinds of information must pass through the network nodes. This project proposes a multi-source heterogeneous information fusion technology [5]. The use of multiple channels to achieve the transmission of various data is the most common. Usually, because each channel's service information processing requirements are different, it is necessary to analyze the access node entering the gateway and determine whether it is safe when transmitting information. This ensures the safe and reliable operation of the universal electrical IoT. Unlike traditional power grid architecture, the universal power grid gateway can provide secure access to all nodes. Intelligent sensing technology collects data from the power grid [6]. The specific power ubiquitous IoT data perception model is shown in Figure 2.1 (image cited in Frontiers in Energy Research, 2022, 10:918998).

3. Multi-level node importance identification method. This paper intends to establish a multi-level identification method of node importance. The importance of nodes at each level is merged to find the nodes

with higher importance. The correlation analysis of the correlation nodes in each network level obtains the reliability and essential measurement. Finally, the critical degree of each node is measured comprehensively. A power communication network composed of M nodes is established. It contains three layers: physical topology, transport, and service. $F_t(i)$ represents the importance of the node i on level t, where $t \in [1,3], i \in [1,M]$ represents its importance. As the $F_t(i)$ level increases, there are more critical nodes i on the t level, giving it a higher subordinate status [7]. Use n_{ti} to determine the membership degree of node i in hierarchy t, then:

$$n_{ti} = \frac{F_t(i) - \min(F_t)}{\max(F_t) - \min(F_t)}$$

After evaluating the critical indicators of a single node, each level of fundamental indicators is proposed to reflect the credibility of each level. Let σ_t represent the underlying metric credibility of level t, and let σ_t conform to the following equation:

$$\sum_{t=1}^{n} \sigma_t = 1$$

where n is the number of logical layers used in the power communication network, in the power system, the importance of power supply is the most direct reflection of power supply interruption to the state of the grid. Since the importance of each business varies greatly, the first consideration should be the level of service [8]. However, if the importance of services in the power communication network is similar or equal, it is necessary to master the corresponding services carried by each node. Therefore, the transport layer is the second consideration. In addition, network services can be placed later if they have the same bandwidth and importance. An adaption-based reliability index for essential measurement is presented to take full advantage of the importance of the three levels:

$$\begin{cases} \sigma_1 = 1 - e^{\delta_{\min} - \delta_{\max}/\delta_{\max}} \\ \sigma_2 = (1-\sigma_1)\left(1 - e^{\lambda_{\min} - \lambda_{\max}/\lambda_{\max}}\right) \\ \sigma_3 = (1-\sigma_1)\, e^{\lambda_{\min} - \lambda_{\max}/\lambda_{\max}} \\ \sigma_1 + \sigma_2 + \sigma_3 = 1 \end{cases}$$

$\delta_{\min}$ and $\delta_{\max}$ are the minimum and maximum importance levels at the service level. $\lambda_{\min}$ and $\lambda_{\max}$ are the minimum and maximum bandwidth of the network layer, respectively. If $\delta_{\max}$ is much larger than $\delta_{\min}$ then σ_1 is very close to 1 . The use of service-level metrics to verify network criticality is entirely correct. Conversely, if $\delta_{\max}$ is close to $\delta_{\min}$ then σ_1 is close to o. The method of service level verification of its critical degree is not highly reliable, so evaluating other levels highlights the reliability. When σ_1 is very close to o, if $\lambda_{\max}$ and $\lambda_{\min}$ are very different then σ_2 is very large. It shows reliable measurements in the transport layer, which can characterize the node's key. On the contrary, when $\lambda_{\max}$ approached $\lambda_{\min}$, it means that the critical degree of the association node is related to the size of the topological layer dimension.

In the multi-level node importance identification model, the measurement of nodes at each level includes two aspects: First, the geometric mean value of each node can be measured at each selected level. The second aspect is to measure the credibility of the indicators [9]. That is, the level of importance of the chosen level is the product of the level of distrust at the bottom of the non-chosen level. The metric for any x logical layer node i is defined as follows ($x \in [1,n], n$ is the total number of logical layers in the power communication network):

$$n_{\psi i} = \sqrt{\prod_{t \in \psi}^{x} n_{t\Omega}}$$

$n_{\psi i}$ measures node $i.\psi$ is the selected logical level. The credibility of the second measure is defined as follows:

$$Q_\psi = \prod_{t \in \psi}^{x} \sigma_t \times \prod_{\Omega \in \Theta}^{n-x} (1 - \sigma_\Omega), \psi \mathrm{I} \Theta = \phi$$

The formula Θ is the logical layer that is not selected. The measurement of a node i in the power communication network of formula (3.5) and (3.6) can be calculated as follows:

$$g_\psi(i) = n_{\psi i} \times Q_\psi$$

$g_\psi(i)$ is a measure of node i in a power communication network. The $2^n - 1$ scheme is adopted when the power grid contains n class logic. Let $G(i)$ be the critical degree of node i, determined by the sum of $g_\psi(i)$ in ψ. To obtain $G(i)$ value, binary array $\alpha, \alpha_t \in \{0, 1\}, t \in [1, n]$ is introduced in this paper. If $\alpha_t = 1$, select t layers from the set ψ. Q indicates that the t layer is unselected [10]. The above $G(i)$ can perform the following calculations:

$$G(i) = \sum_{[\alpha]\neq 0} \left[[\alpha] \sqrt{\prod_{\alpha_t=1}^{[\alpha]} n_{ti}} \times \prod_{\alpha_t=1}^{[\alpha]} \sigma_t \times \prod_{\alpha_t=0}^{n-[\alpha]} (1 - \sigma_\Omega) \right]$$

σ_t is based on t level measurement reliability; $[\alpha]$ is the number of 1 in series α. As $G(i)$ increases, there will be more critical nodes.

4. Access node identification technology of gateway. With the continuous development of the Internet of Things technology, its security issues have attracted more and more attention. A credible evaluation model oriented to user behavior is studied to provide reliable technical support for promoting the healthy development of the Internet of Things. Access nodes are divided into several levels based on an assessment of trustworthiness [11]. Each level of resources is stored in the corresponding security zone of the trust level to prevent hackers from stealing or cracking the high-performance service gateway. Observe the change in the trust level between users according to the interaction evaluation list between users so that users with high trust can interact with each other in different areas. This can improve the network's security performance and prevent data leakage in the power system. Use the A-Node control mode to re-identify nodes that do not meet the security requirements [12]. It is also excluded to reduce the possibility of low-performance nodes attacking high-performance nodes.

All-access nodes associated with the universal power grid access gateway have security risks such as viruses and trojans. A secure access node identification model is necessary to prevent malicious intrusion [13]. The preemptive loading method is adopted to remove the "hidden channel's security effectively." It promotes the whole network's operation and achieves the gateway's secure access requirement. Identifying the secure access nodes of the universal power grid gateway is a vital part of improving the security defense capability of the power grid and ensuring the safety level of the power grid operation.

Due to the network's large number of access nodes and diverse service requirements, it is difficult to grasp its security accurately. By analyzing the reliability of the access node, the network control model of the access node is established to realize the identification of the access node. To obtain the best access control results, it is necessary to organically integrate the functions of access node automatic update and access control [14]. A gateway access node control model based on access control is proposed in this paper. The primary security monitoring method is used to realize the security check of the access node. Implement authorization control for some nodes with low trust. The specific function design of the gateway access node control model is shown in Figure 4.1.

Analyzing the attached Figure 4.1 shows that in the ubiquitous Internet of Things, the core of network monitoring is the host's network behavior and the host's status, and the background database realizes the exchange of monitoring information. The method uses the monitoring background database and identifies the access nodes in the network by analyzing the confidence of access nodes. An access node identification model for defect detection is proposed [15]. For the access nodes that have completed the preliminary identification, the vulnerability detection of the network is started. The work module is divided into five parts. First, the vulnerability database is modeled. Then, a console panel was added for the user terminal device. Then, scan access nodes. Scan the currently active knowledge base. The vulnerability scanning process is shown in Figure 4.2.

During vulnerability detection, it is necessary to ensure that the credibility database of the access node can be updated in time and it can identify whether the access node has security risks. The nodes identified for the

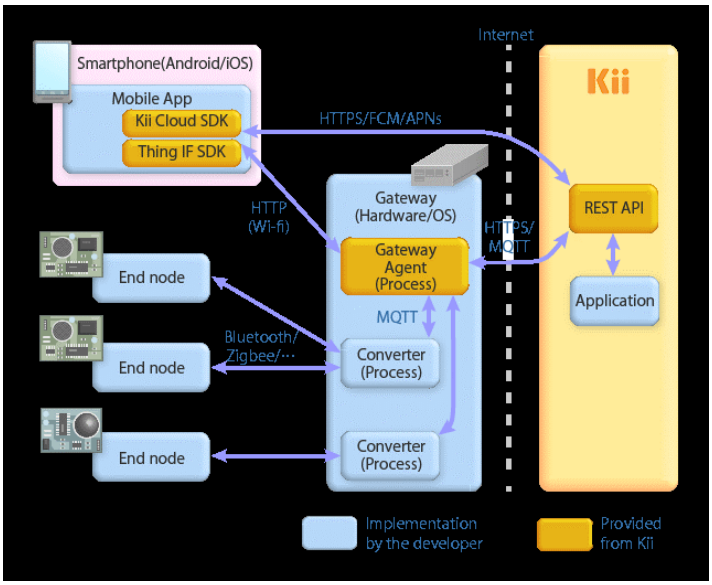

Fig. 4.1: *Functional design of Gateway Access Point Control Model.*

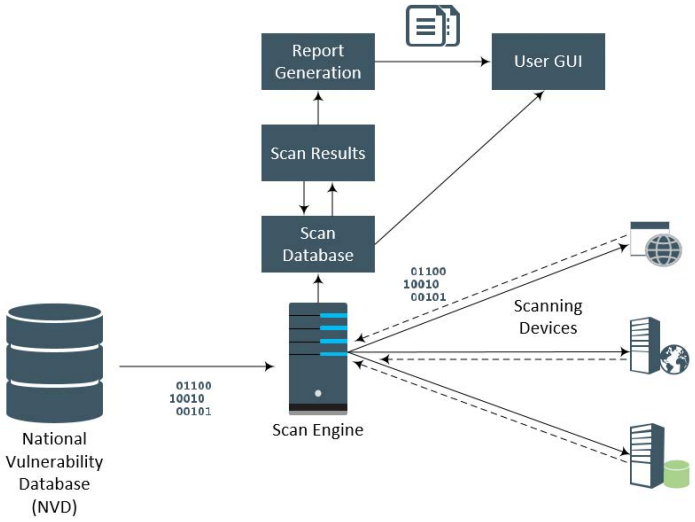

Fig. 4.2: *Vulnerability scanning process.*

first time are re-detected using the network vulnerability scanning technology [16]. The process is to process the access node according to the access request and determine its credibility change. After virus detection is complete, a detection report is sent to the background. Finally, the trusted access function is introduced to monitor the degree of trust of IoT network access nodes. By analyzing the behavior of access users, collect their business requirements. And according to the required information to generate the resolved results.

5. Simulation test. Simulation software is used to test the security of the proposed universal grid gateway. The universal power grid gateway is simulated by simulation software. The model is verified by adding different access nodes to the network. This project intends to adopt two common recognition patterns: network access recognition pattern based on near neighbor discovery and network access recognition model based on D-S

Table 4.1: *Comparison of precision under fixed parameters.*

Times	**This article model (%)**	**model 1 (%)**	**model 2 (%)**
1	97.46	73.04	54.88
2	89.36	74.43	49.33
3	89.94	71.20	51.05
4	98.86	73.94	61.08
5	92.74	77.83	54.23
6	93.49	78.64	53.53
7	91.58	76.17	53.09
8	99.32	76.90	50.70
9	93.78	73.14	52.07
10	91.18	72.85	57.93

evidence. The test is carried out under the same working conditions. According to the identification results, the applicable range of the model is determined [17]. The accuracy method is used to test the validity of access node identification. The nodes whose trustworthiness meets the entry access conditions are called secure nodes, while the opposite nodes are considered malicious. Precision, therefore, measures the percentage of secure nodes in each accessed node. So, the expression for precision is

$$P_{\text{precision}} = \frac{S}{Q}$$

where Q is the access node and S is the number of secure access nodes. In the simulation program, 1000 access nodes were set up, and ten experiments were carried out. Results for accuracy are shown in Table 5.1. Compared with the two conventional recognition methods, the proposed method can obtain better recognition results under the same parameters [18]. The accuracy of the model proposed in this paper is 93.77%, and the accuracy of the two classical prediction methods is 53.79% and 74.81%, which are 39.98% and 18.95% higher than the existing methods. Therefore, under the given parameter conditions, the model gateway constructed in this paper has a much better security access node identification effect.

On the premise that there are already 1000 access nodes, the number of nodes is gradually increased by 200. The influence of these three modes on the recognition of access nodes is shown in Figure 5.1. When the overall scale of the access network increases, its accuracy rate is maintained at a relatively stable level [19]. Its accuracy is significantly higher than that of the two conventional models. Its accuracy rate can be maintained at the level of 0.85-0.9. The accuracy of classical mode 1 is 0.65-0.7. Classic Mode 2 had the lowest accuracy at 0.5; therefore, when the number of networks increases, the accuracy of the proposed algorithm model can be increased by 20% and 38%, respectively.

The expansion rate of the network is 200 based on the original number of nodes. The results of the accuracy of these three methods changing over time are shown in Figure 5.2. When the number of malicious networks in the network increases, the search accuracy of this method also changes slightly but still maintains a relatively stable level. However, the accuracy of the two classical prediction methods has been dramatically reduced. The results show that the accuracy of model 1 is reduced from 0.7 to 0.43. 2 mode is reduced from 0.5 to 0.4. The universal network gateway secure access node identification method proposed in this project improves accuracy by 46% and 49%, respectively, when the number of malicious nodes increases to identify gateway secure nodes efficiently.

5. Conclusion. This project will establish a network-based gateway security access node screening model based on the universal electric power of the Internet of Things and conduct experimental verification. It is expected that through the research of this project, the extensive use of the Internet of Things in the power system will be promoted, and the operating status of the overall power system and the identification accuracy of network nodes will be improved. It lays an excellent theoretical and practical foundation for the innovative development of power systems. Although it can be seen from the experiment that the proposed recognition

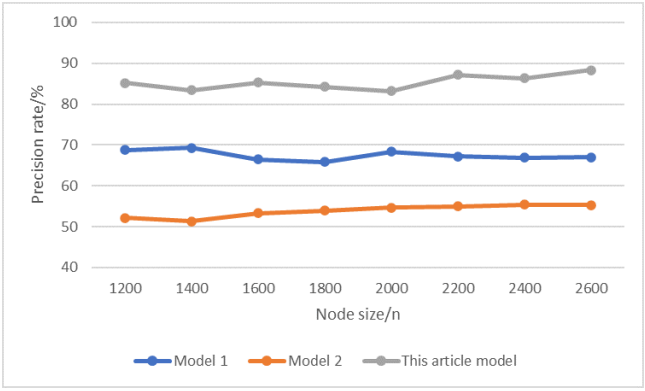

Fig. 4.3: *Comparison of accuracy when the overall node size increases.*

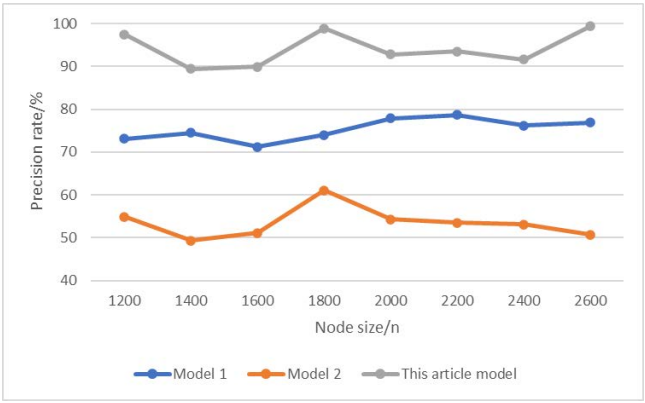

Fig. 4.4: *Comparison of accuracy in the state of malicious node size increase.*

method has achieved good results in practice, there are still many shortcomings which need to be further studied.

REFERENCES

[1] Guzs, D., Utans, A., Sauhats, A., Junghans, G., & Silinevics, J. (2022). Resilience of the Baltic power system when operating in island mode. IEEE Transactions on Industry Applications, 58(3), 3175-3183.
[2] Ankit, A., Liu, Z., Miles, S. B., & Choe, Y. (2022). Us resilience to large-scale power outages in 2002–2019. Journal of safety science and resilience, 3(2), 128-135.
[3] Jayalath, J. A. R. C., & Premaratne, S. C. (2021). Analysis of key digital technology infrastructure and cyber security consideration factors for fintech companies. International Journal of Research Publications, 84(1), 128-135.
[4] Ragusa, A., Sasse, H. G., Duffy, A., & Rubinstein, M. (2021). Application to real power networks of a method to locate partial discharges based on electromagnetic time reversal. IEEE Transactions on Power Delivery, 37(4), 2738-2746.
[5] Konaszczuk, W. (2021). Cybersecurity Threats in the Sectors of Oil, Natural Gas and Electric Power in the Context of Technological Evolution. Studia Iuridica Lublinensia, 30(4), 333-351.
[6] Herr, T. (2021). Cyber insurance and private governance: The enforcement power of markets. Regulation & Governance, 15(1), 98-114.
[7] Brown, O., Power, N., & Conchie, S. M. (2021). Communication and coordination across event phases: A multi-team system emergency response. Journal of Occupational and Organizational Psychology, 94(3), 591-615.
[8] Nova, K. (2022). Security and Resilience in Sustainable Smart Cities through Cyber Threat Intelligence. International Journal of Information and Cybersecurity, 6(1), 21-42.
[9] Bai, F., Cui, Y., Yan, R., Saha, T. K., Gu, H., & Eghbal, D. (2022). Frequency response of pv inverters toward high renewable

penetrated distribution networks. CSEE Journal of Power and Energy Systems, 8(2), 465-475.
[10] Niu, H., Lin, Z., An, K., Liang, X., Hu, Y., Li, D., & Zheng, G. (2022). Active RIS-assisted secure transmission for cognitive satellite terrestrial networks. IEEE Transactions on Vehicular Technology, 72(2), 2609-2614.
[11] Jha, R. K. (2023). Cybersecurity and Confidentiality in Smart Grid for Enhancing Sustainability and Reliability. Recent Research Reviews Journal, 2(2), 215-241.
[12] Cecilia, A., Sahoo, S., Dragičević, T., Costa-Castelló, R., & Blaabjerg, F. (2021). On addressing the security and stability issues due to false data injection attacks in DC microgrids—An adaptive observer approach. IEEE Transactions on Power Electronics, 37(3), 2801-2814.
[13] Zhang, Z., Deng, R., Yau, D. K., Cheng, P., & Chow, M. Y. (2022). Security enhancement of power system state estimation with an effective and low-cost moving target defense. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 53(5), 3066-3081.
[14] Spring, J. M., & Illari, P. (2021). Review of human decision-making during computer security incident analysis. Digital Threats: Research and Practice, 2(2), 1-47.
[15] Chowdhury, N. (2021). CS measures for nuclear power plant protection: A systematic literature review. Signals, 2(4), 803-819.
[16] Yang, T., Liu, Y., & Li, W. (2022). Attack and defence methods in cyber-physical power system. IET Energy Systems Integration, 4(2), 159-170.
[17] Boersma, K., Ferguson, J., Groenewegen, P., & Wolbers, J. (2021). The dynamics of power in disaster response networks. Risk, Hazards & Crisis in Public Policy, 12(4), 418-433.
[18] Schmitz-Berndt, S., & Schiffner, S. (2021). Don't tell them now (or at all)–responsible disclosure of security incidents under NIS Directive and GDPR. International Review of Law, Computers & Technology, 35(2), 101-115.
[19] Kammersgaard, T. (2021). Private security guards policing public space: using soft power in place of legal authority. Policing and society, 31(2), 117-130.

Edited by: Zhigao Zheng
Special issue on: Graph Powered Big Aerospace Data Processing
Received: Dec 4, 2023
Accepted: Dec 25, 2023