

Article

A Bayesian-Attack-Graph-Based Security Assessment Method for Power Systems

Lu Chen ^{1,2,*}, Tao Zhang ^{1,2}, Yuanyuan Ma ^{1,2}, Yong Li ^{1,2}, Chen Wang ^{1,2}, Chuan He ^{1,2}, Zhuo Lv ^{3,4} and Nuannuan Li ^{3,4}

¹ State Grid Smart Grid Research Institute Co., Ltd., Nanjing 210003, China; zhangtao@geiri.sgcc.com.cn (T.Z.); mayuanyuan@geiri.sgcc.com.cn (Y.M.); liyong@geiri.sgcc.com.cn (Y.L.); wangchen@geiri.sgcc.com.cn (C.W.); hechuan@geiri.sgcc.com.cn (C.H.)

² State Grid Laboratory of Power Cyber-Security Protection and Monitoring Technology, Nanjing 210003, China

³ State Grid Henan Electric Power Research Institute, Zhengzhou 450000, China; lvzhuo@ha.sgcc.com.cn (Z.L.); linuannuan@ha.sgcc.com.cn (N.L.)

⁴ State Grid Henan Electric Power Company, Zhengzhou 450000, China

* Correspondence: chenluchina@aliyun.com

Abstract: In today's highly advanced information technology environment, modern network and communication technologies are widely used in monitoring and controlling power systems. These technologies have evolved significantly. They now form a high-performance digital system known as the cyber-physical power system. However, vulnerabilities in communication networks present growing threats to these systems. This paper seeks to enhance the accurate assessment of the security posture of cyber-physical power systems by inferring attackers' intentions. A threat modeling approach based on Bayesian attack graphs is presented, employing Bayesian networks to define and evaluate potential threats that attackers could pose to different system infrastructures. The paper initially conducts a qualitative analysis of the system's threats, constructing a directed graph structure and establishing conditional probability tables among nodes based on prior knowledge. Subsequently, methods are developed to compute the threat levels at different system nodes using real-time detected attack events. Further analysis methods and security assessment metrics are also developed to identify attack paths and quantify system security. Finally, a Bayesian attack graph is constructed in accordance with the system's structure. In practical scenarios, the attack path analysis method can predict the most vulnerable attack paths, while the absolute values of the security assessment metrics indicate the overall risk level of the system.

Keywords: cyber-physical systems; Bayesian attack graph; threat modelling; power system security; vulnerability assessment



Citation: Chen, L.; Zhang, T.; Ma, Y.; Li, Y.; Wang, C.; He, C.; Lv, Z.; Li, N. A Bayesian-Attack-Graph-Based Security Assessment Method for Power Systems. *Electronics* **2024**, *13*, 2628. <https://doi.org/10.3390/electronics13132628>

Academic Editor: Elio Chiodo

Received: 15 May 2024

Revised: 29 June 2024

Accepted: 2 July 2024

Published: 4 July 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Modern power grids are critical infrastructure, and any threats to them could significantly impact national security and economic stability. Integrating modern network communication technology into power systems enhances monitoring and control functions [1]. However, this incorporation increases the likelihood of cyber threats, raising the risk of catastrophic failures. If the vulnerabilities of the system are attacked, it will threaten the safe and stable operation of the power systems and cause serious consequences [2]. The new generation of power systems, which intertwine traditional power grids with modern network communication technologies, are regarded as highly interconnected and interdependent infrastructure [3–5]. Any component failure can significantly affect the entire power system [6].

Standardized communication protocols reveal vulnerabilities. These vulnerabilities affect power systems significantly, allowing attackers to gain unauthorized access and control over assets [7]. These new power systems comprise both traditional power grid

infrastructure and communication networks for monitoring and control. Substations communicate with regional control centers using Ethernet protocols, while control centers exchange information via inter-control center protocols and communicate with transmission operators through Ethernet routers. In this context, intruders can exploit vulnerabilities in control centers or substations to gain administrator privileges over human–machine interfaces. With this access, they can manipulate control commands to operate circuit breakers in the physical power system, leading to imbalances between power generation and load that cause grid instability [8].

For example, the Stuxnet attack in 2010 exploited programmable logic controllers that controlled centrifuges, causing equipment failures and severely damaging Iran’s nuclear facilities. In 2015, a coordinated cyberattack caused a massive power outage in Ukraine, affecting hundreds of thousands of people. These incidents took advantage of vulnerabilities in firewalls and communication protocols within power systems. Due to their critical positions and weak defense mechanisms, these network vulnerabilities are attractive to hackers and pose significant risks to the safe and stable operation of power grids. Therefore, assessing and analyzing the vulnerabilities of cyber–physical power systems under cyberattacks is essential, enabling the effective identification of weak nodes and the rational allocation of defense resources.

In recent years, researchers worldwide have explored this issue and proposed various assessment methods. Wu [9] designed a network attack selection model based on attack costs. By analyzing these costs, they identified network attacks with higher probabilities of success and provided corresponding countermeasures, reducing cybersecurity risks. However, their method overlooked the attack gains those attackers consider in practice. Sun [10] combined Markov chains and attack graphs to assess network risks, quantifying atomic attack success probabilities based on vulnerability disclosure status, available attack methods, and tools. They calculated node risk values accordingly. Hu [11] converted attack graphs into absorbing Markov chains and quantified state transition probabilities using the CVSS vulnerability scoring system, thereby determining node probabilities. Although these methods are feasible, they overlook that attackers are intelligent decision-makers who consider both attack costs and gains. Additionally, as these methods do not account for the impact of detected attack events on node probabilities, they can only provide static assessments and cannot dynamically evaluate risks.

Xie [12] considered attack events while analyzing network security with Bayesian networks but did not calculate the posterior probabilities of nodes with observed attack events. Poolsappasit [13] used observed node states in Bayesian networks as attack evidence to compute posterior probabilities, dynamically assessing network risk and providing administrators with real-time security insights. Chen [14] used observed attack events to deduce the probability of specific attacks but only discussed the impact of observed attack events on the posterior probabilities of directly affected nodes, neglecting the influence on related nodes. Gao [15] comprehensively considered the effect of attack events on posterior probabilities when assessing network risk using Bayesian attack graphs but did not analyze how attack costs and benefits affected node probabilities. Ma [16] quantified node probabilities based on attack pressure and unknown threats, improving assessment accuracy, but overlooked cases where node relationships are “OR”.

Risk analysis involves inherent uncertainties that incorporate aspects such as the complexity of the system, parameter randomness, the risk model applied, and human subjectivity [17]. Based on the above principles, this paper introduces a novel threat modeling approach tailored for power system infrastructures. Unlike typical methods that overlook the economic motivations behind attacks, our model innovatively incorporates the importance of assets and the cost implications of launching attacks. This dual consideration allows for a more realistic estimation of an attacker’s probability of initiating an attack, directly addressing the gap in existing approaches that often simplify attacker behavior to technical factors alone.

Further advancing the field, we have developed a method that dynamically calculates the threat level on different system nodes using real-time detected attack events. This approach enhances the adaptability of security assessments, allowing for real-time updates and more accurate risk evaluations compared to static models that fail to capture the fluid nature of cyber threats.

Additionally, our work enhances traditional risk assessments by introducing attack path analysis methods and security evaluation metrics that provide quantifiable indicators following the completion of risk analysis, enabling a detailed evaluation of system vulnerabilities and defenses. These innovations not only help in identifying high-risk attack paths but also facilitate a deeper understanding of systemic vulnerabilities through the comparison of security assessment values based on prior and posterior probabilities. By integrating these elements, the proposed method significantly refines the accuracy and relevance of security assessments, providing a comprehensive tool for power system protection.

The primary application of the Bayesian attack graph methodology developed in this paper is to enhance the security assessment of cyber-physical power systems. These systems, integral to the infrastructure of modern power grids, are increasingly susceptible to sophisticated cyberattacks that can disrupt their operation and stability.

Our approach utilizes Bayesian attack graphs to model potential attack paths and quantify the likelihood of successful exploits, enabling system operators to predict and mitigate the most probable threats. By integrating this model into regular security assessments, operators can dynamically evaluate the system's vulnerability to various attack scenarios. This proactive analysis helps in prioritizing security measures and allocating resources more effectively to protect critical infrastructure components.

The Bayesian attack graph method offers a systematic way to assess risk by considering both the likelihood of attack vectors and the potential impact of successful breaches. This dual focus is crucial for maintaining not just the operational integrity but also the safety of power systems which are essential for national security and economic stability.

The remainder of this paper is organized as follows. Section 2 discusses the technical methods involved in the proposed approach. Section 3 describes the novel power system model used for threat analysis. Section 4 provides a detailed simulation of the proposed solution's results. Finally, Section 5 concludes this paper.

2. Power System Cyber Security Analysis and Modelling

Malicious cyberattacks targeting power systems typically progress through multiple stages, with each stage exploiting vulnerabilities in various system assets. Beyond the initial attack, subsequent stages depend on successfully compromising specific assets within the system. This dependence implies that network intrusions can be modeled using directed graphs, where nodes represent assets and attack actions, and directed edges signify the dependencies between them. Thus, by analyzing the topology and vulnerabilities of the system, a corresponding Bayesian attack graph can be constructed. The process for constructing a Bayesian attack graph for a specific system is illustrated in the diagram. The lowest layer consists of the physical entities, including primary electrical equipment such as generators, transformers, transmission lines, and loads. These components are electrically interconnected within the physical layer, forming the backbone of the power system that directly handles the generation, transmission, and distribution of electrical energy.

As shown in Figure 1, this illustrates the process of constructing a Bayesian attack graph. The first step involves analyzing the network topology and vulnerability information of the system to establish the structure of the Bayesian attack graph. Subsequently, by integrating CVSS metrics and expert knowledge, the probabilities of vulnerability exploitation and attack execution are assessed, resulting in the conditional probability distribution of the nodes. Once the quantification of node information is completed, a complete Bayesian attack graph is obtained.

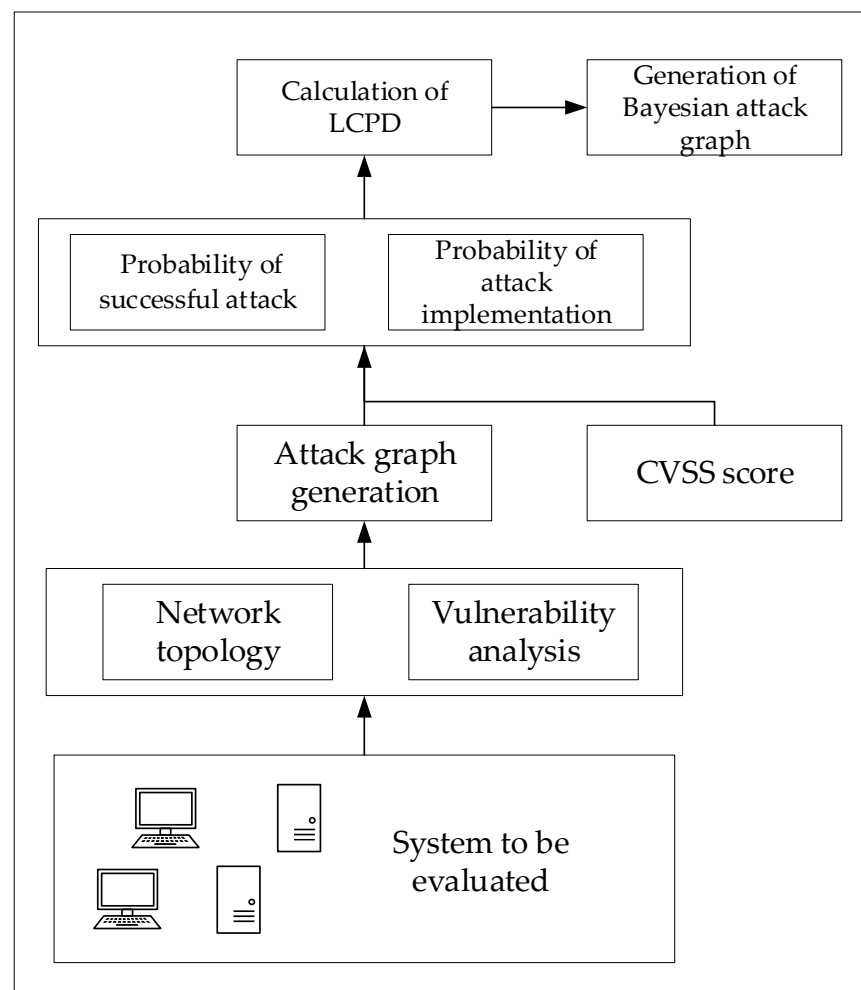


Figure 1. Bayesian attack graph generation framework.

Therefore, this section will conduct a cybersecurity analysis of the electrical power system, introducing the types of cyberattacks that may exist within the system. Following this, the basic definition of the Bayesian attack graph for the targeted power system is provided. Finally, a node information quantification method based on CVSS scoring metrics is proposed, facilitating the construction of the Bayesian attack graph.

2.1. Power System Network Security Analysis

Modern power grids are exemplary cyber–physical systems (CPSs), intricately weaving together electrical infrastructure and communication technology. As depicted in Figure 2, the hierarchical structure of the power CPS is meticulously outlined from the control centers to the physical devices.

At the topmost layer are the control centers, encompassing distribution main stations, SCADA servers, and Management Information System (MIS) servers [18]. These centers form the neural network of the power CPS, responsible for processing and managing data across the entire grid, monitoring the operational status, and ensuring the stability and security of the power supply.

Beneath this is the power communication network layer, composed of various communication devices and protocols, such as routers, smart meters, and actuators. This layer facilitates the transmission of data, including measurement information and control commands, between the control centers and distributed substations, ensuring seamless communication within the system.

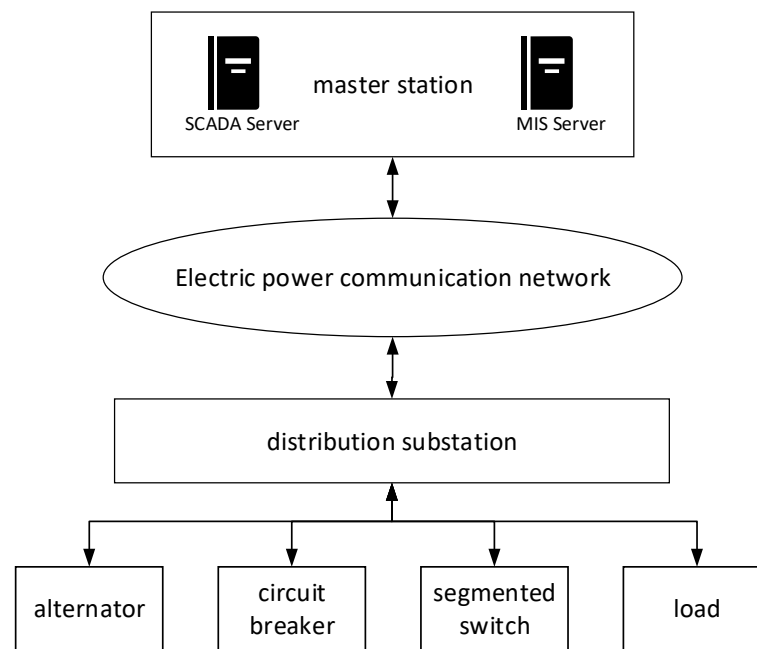


Figure 2. Hierarchical structure of the power CPS.

Further down is the distributed substation layer, equipped with secondary devices like Remote Terminal Units (RTUs) and Feeder Terminal Units (FTUs). These units act as the interface between the physical and information layers, collecting real-time data from the grid and executing control commands from the information layer, playing a crucial role in regulating the operation of the power system.

The lowest layer consists of physical entities, including primary electrical equipment such as generators, transformers, transmission lines, and loads. These components are electrically interconnected within the physical layer, forming the backbone of the power system that directly handles the generation, transmission, and distribution of electrical energy.

Building upon the integrated communication technologies within the power CPS, the system is a multi-layered distributed network, where each subsystem interacts and coordinates through fiber optic communications and wireless transmission methods. Sensors embedded within primary power equipment continuously sample operational data from the power system. These data are digitized by measuring and control units and transmitted up the communication network to the main station's measurement data management system. The central station servers then perform real-time online calculations based on the received grid operational data and issue control commands to regulate power generation equipment. These control commands are relayed through the communication network to specific devices, where intelligent control units execute operations according to the instructions provided.

Network attacks on power CPS systems can be divided into WAN and NAN attacks. Wide Area Network (WAN) communication has a broad coverage (up to 100 km), with a data transmission frequency ranging from 10 Mbit/s to 1 Gbit/s. It supports real-time monitoring and protection in power systems and provides a communication pathway between NANs and control centers, thus serving as the backbone of smart grid networks. Power applications like SCADA telemetry, EMMS energy management, WAMS phasor measurement unit (PMU) data processing, and data exchange between substations and control centers rely on WAN communication [19]. Typical WAN attack targets include generation and control equipment. In substation automation, WAN attacks can occur via VPNs, dial-up networks, wireless networks, remote login programs, or Trojan programs on unidentified devices. Infiltration methods include repetitive dialing, scanning, communication monitoring, and password cracking. Such attacks could lead to the loss or tampering of system information, causing secondary equipment misoperation or failure, potentially

resulting in equipment damage, line overloads, load losses, and system instability. In extreme cases, this could trigger large-scale cascading failures, leading to severe economic losses [20].

Neighborhood Area Networks (NANs) support data exchange between WANs and users within a range of approximately 10 km, with data transmission rates from 100 kbit/s to 10 Mbit/s. NANs facilitate bidirectional data transmission between user devices and data concentrators or substations, enabling services like remote metering, usage control, and field equipment monitoring through the metering network. Typical NAN attack targets include power substations and distribution centers, and attacks can be carried out directly through substations or secure access gateways. Since NANs connect users to WANs, their network security is crucial to the entire smart grid. NAN network attack detection can leverage intrusion detection systems based on support vector machines and artificial intelligence methods [21]. Scholars also suggest adopting more sophisticated authentication mechanisms to reduce NAN network attack risks.

Furthermore, on the user side of power systems, attackers can reverse-engineer easily accessible user-side equipment (e.g., smart meters and communication hardware) to identify vulnerabilities for targeted attacks. Strengthening authentication mechanisms is also an effective preventive measure against these attacks.

In power systems, network attacks primarily exploit security vulnerabilities to infiltrate information devices, gaining control over functional nodes and progressively compromising the information system to disrupt the normal operation of intelligent electronic devices. This could ultimately cause system failures and disrupt the power grid's normal functioning, thereby achieving cross-domain attacks from the information to the physical domain. As new applications and smart devices increasingly connect to power CPS systems, substations and distribution centers face more NAN network attacks. Therefore, this paper mainly investigates network attacks on substation control center local area networks.

2.2. Definition of Bayesian Attack Graphs

Probabilistic graphical models effectively and succinctly represent relationships between variables and offer powerful tools for reasoning under uncertainty. They have become a popular research area in artificial intelligence and machine learning in recent years. Currently, probabilistic graphical models have been successfully applied in various fields, including image analysis, biomedical studies, and computer science. To perform uncertain reasoning using probabilistic graphical models, one must first construct the model using domain knowledge. Probabilistic graphical models combine graph theory and probability theory to compactly describe multivariate statistical relationships. Different representations exist, such as Bayesian networks, Markov networks, chain graphs (CGs), temporal models (TMs), and probabilistic relational models (PRMs). Although these representations vary, they all aim to factorize joint probability distributions by assuming conditional independence, simplifying the representation and inference process. Due to their ability to reflect the uncertainty of attack behaviors effectively, Bayesian networks are commonly used to model and detect distributed threats in threat modeling.

Bayesian networks consist of nodes and directed edges. The directed edges indicate dependencies between nodes, which may represent logical relationships such as causality. A directed edge from node 1 to node 2 indicates that the probability distribution of node 2 is influenced by node 1. If no path exists between two nodes, they are considered probabilistically independent. In threat modeling, nodes represent resources and attacks, while directed edges illustrate causal relationships. A directed edge from an attack node to a resource node suggests that the resource may be at risk of this attack, meaning it could be compromised if the attack is launched.

To model vulnerabilities in power CPS systems using Bayesian attack graphs, we assume that attackers have one or multiple potential targets, such as compromising the confidentiality, integrity, or availability of certain system resources. Various smart devices within power CPS systems contain exploitable vulnerabilities, some of which can be

directly leveraged by attackers while others require a certain level of privilege [22]. Thus, in constructing a Bayesian network, resource nodes may not represent a complete device but rather a specific privilege within a device. Attacking this privilege implies that the corresponding vulnerability is being exploited. We assume that the probability of launching an attack depends on its difficulty and potential rewards, while its success rate relies on how easily a vulnerability can be exploited. The attack initiation probabilities constitute the local conditional probability distribution (LCPD) tables of attack nodes, while the attack success probabilities form the LCPD tables of resource nodes.

To quantify threats using Bayesian attack graphs, one must first establish a structural model based on information such as the power network environment, terminal assets, network connectivity, and threat information. Next, a risk assessment system is constructed, and conditional probability tables are provided for each node, forming a complete Bayesian network. Finally, based on the prior probabilities of threat nodes and the conditional probability tables of each node, one can compute the potential changes in core assets resulting from any given threat.

A Bayesian network is a directed acyclic graph with conditional probability tables, defined as a five-tuple $B_{AG} = \{S, A, E, R, T\}$ with specific meanings as follows.

1. $S = S_{ext} \cup S_{int} \cup S_{ter}$, S is the set of resource nodes, comprising external attack initiation nodes S_{ext} , attribute state nodes S_{int} , and final attribute state nodes S_{ter} . The nodes have binary values (true/false, 1/0). When false, the attacker lacks specific attack resources or access privileges; when true, the attacker has such resources or privileges. For a node S_i , $P(S_i)$ denotes its accessibility probability, indicating the likelihood that the node has been compromised.
2. $A = \{A_i | i = 1, 2, \dots, n\}$ is the set of attacks in the graph, representing exploitation of asset vulnerabilities. Both parent and child nodes of an attack node are resource nodes. Attack nodes also have binary values. For an attack node A_i , $P(A_i)$ indicates the probability of launching this attack.
3. $E = \{E_i | i = 1, 2, \dots, n\}$ is the set of directed edges in the graph, representing dependencies between nodes. An edge from an asset to an attack node indicates that the attack depends on its parent resource node. An edge from an attack to a resource node indicates that the attack exploits a specific vulnerability of the asset.
4. R represents the dependency of any node with its set of parent nodes. The relations can be either AND (all parents must be true) or OR (at least one parent is true).
5. T is the node's local conditional probability distribution (LCPD) table. Attack node tables depend on attack initiation probabilities, and resource node tables depend on the probability of successful exploitation of their vulnerabilities.

2.3. Quantification of Node Information

After constructing the Bayesian network, it is essential to generate conditional probability tables for each intermediate node and calculate the prior probabilities for the initial attack nodes. With these tables and Bayes' theorem, we can compute the conditional probabilities of each node, thereby assessing the network's risk values and predicting potential attack behaviors in advance. Since the Bayesian network in this study is constructed based on the exploitation relationships between vulnerabilities, the network edges represent the vulnerabilities exploited to achieve the attacks. Thus, the conditional probability tables of the Bayesian attack graph are derived from the relevant vulnerability information.

Conditional probability is the likelihood of event B occurring given that event A has already happened. In a Bayesian network, the conditional probability of a node indicates the likelihood of an attack happening, provided that certain attack conditions are met. A vulnerability's severity affects the probability of it being exploited. If the vulnerability level is high, exploitation is more challenging, and thus, less likely. Conversely, if the vulnerability is easily exploited, the success probability of the attack increases. In this study, the Common Vulnerability Scoring System (CVSS) is used to assess vulnerabilities [23], converting these scores into probabilities.

Exploitability, the CVSS sub-item is defined as follows:

$$Exploitability = 8.22 \cdot AV \cdot AC \cdot PR \cdot UI \quad (1)$$

In the CVSS (Common Vulnerability Scoring System) framework, the Attack Vector (AV) metric assesses how a vulnerability can be exploited remotely; a higher score indicates that an attacker can exploit the vulnerability from a more remote location. The Attack Complexity (AC) metric evaluates the complexity of the attack; a higher score signifies that the attack is easier to perform. The Privileges Required (PR) metric determines the level of privileges necessary for an attack; a higher score means lower privileges are needed. The User Interaction (UI) metric measures the degree of user interaction required for an attack; a higher score indicates less user interaction is necessary. Table 1 lists the values of these metrics at different levels.

Table 1. Evaluation Indicators for Basic Metrics Groups.

Norm	Hierarchy	Score
Access Vector	Physical/Local/Adjacent Network/Network	0.2/0.55/0.62/0.85
Access Complexity	High/Low	0.44/0.77
Privileges Required	High/Low/None	0.5/0.68/0.85
User Interaction	Required/None	0.62/0.85

The sub-item “Exploitability” in the CVSS metrics involves calculating the product of the individual scores for Attack Vector (AV), Attack Complexity (AC), Privileges Required (PR), and User Interaction (UI), and then multiplying this product by a constant factor of 8.22. We can refer to it to define the vulnerability exploitability probability. However, considering the definition of probability, which must fall within the interval [0, 1], it is necessary to adjust this constant to fit within these bounds.

To accommodate this requirement, the vulnerability exploitability probability (the attack success probability) can be defined as follows:

$$P_e = 2 \cdot AV \cdot AC \cdot PR \cdot UI \quad (2)$$

For the attacker, the probability of attacking a node depends on the ratio of the attack cost to the attack benefit. The cost is related to the difficulty of exploiting the node’s vulnerability, and it is characterized using the base metrics group. The benefit depends on the value the attacker gains from compromising the asset. The attack benefit is defined in Table 2.

Table 2. Attack Gain.

Metric	Value
information leakage	0.3
remote registration	0.55
Authentication bypass	0.65
limited access	0.85
full competence	1

Considering both attack costs and benefits, the probability of an attack occurring is defined as follows:

$$P_a = AC \cdot AV \cdot Value \quad (3)$$

3. Design of the Security Assessment Methodology

In the specific context of power systems, after generating a Bayesian attack graph, it is essential to calculate the conditional probability tables for each node based on prior knowledge to quantify node information. Furthermore, this chapter introduces a static

risk analysis method based on prior probabilities and a dynamic risk analysis method based on posterior probabilities. To better understand the attacker's estimated intent and evaluate the overall risk status of the system, an attack path analysis method and security assessment metrics are proposed.

3.1. Static Risk Analysis

Security risk refers to the potential that a specific threat could exploit asset vulnerabilities, leading to damage or disruption. Threat risk assessment is foundational for providing threat feedback and implementing security measures. This study proposes a probabilistic graph-based threat risk assessment algorithm using a Bayesian network model. By analyzing the initial values of threat nodes and the topology of attack paths, the algorithm calculates the probability of each resource node entering a risky state, along with other related information. The results can vary depending on the focus of the system's security goals, with each boundary threat node's value determined by the system's actual conditions.

If no active attack is detected in the system but exploitable vulnerabilities exist in the network, risk quantification of network assets and the overall network environment can be achieved by evaluating the likelihood of vulnerability exploitation and the importance of assets. Based on the quantified risk values, one can predict which targets attackers are most likely to pursue, allowing security personnel to take appropriate defensive measures.

Upon completing the construction of the Bayesian network structure and calculating the conditional probabilities using prior knowledge, it is only necessary to specify the probability of an initial attack node launching an attack to compute the prior probabilities of all nodes. This prior probability represents either the probability of the resource represented by the node being compromised by an attacker or the probability of the attack being initiated by the node. In our designed Bayesian attack graph, the parent node of a resource node is always an attack node, and the parent node of an attack node is always a resource node. Therefore, we need to discuss separately the methods for calculating the prior probabilities of these two types of nodes. For any resource node S_k , assume it has n parent attack nodes, denoted as e_i for convenience. Further, $P(e_i)$ represents the probability of the attacker launching that attack, and P_{ei} is the probability of the attack being successful, which is the exploitability probability defined earlier. The calculation formula for the prior probability of the node depends on its dependency relationship R with its parent nodes. The formulas for calculating the prior probability of the resource nodes under different dependency relationships are as follows:

$$P(S_k) = \begin{cases} \prod_{i=1}^n P_{ei} \cdot P(e_i), R = AND \\ 1 - \prod_{i=1}^n [1 - P_{ei} \cdot P(e_i)], R = OR \end{cases} \quad (4)$$

This formula uses the prior probabilities of the parent nodes, which are the attack nodes. The prior probability of an attack node A_h is dependent on the prior probabilities of its parent resource nodes. For any attack node A_h , assume it has m parent resource nodes, denoted as a_j for convenience. Further, $P(a_j)$ represents the probability of the attacker compromising that resource node, and P_{aj} is the probability of the attacker launching further attacks after occupying that resource, which is the attack occurrence probability defined earlier. The formula for calculating the prior probability of the attack node depends

on its dependency relationship R with its parent nodes. The formulas for calculating the prior probabilities of attack nodes under different dependency relationships are as follows:

$$P(A_h) = \begin{cases} \prod_{i=1}^n P_{aj} \cdot P(a_j), R = AND \\ 1 - \prod_{i=1}^n [1 - P_{aj} \cdot P(a_j)], R = OR \end{cases} \quad (5)$$

The steps to use the Bayesian network model for threat risk assessment are as follows:

Input: Attack graph $AG = (S, A, E, R, T)$, as previously defined;

Output: Static risk assessment probabilistic graph $SAG = (S, A, E, R, T, P_1)$, where P_1 is the set of prior probabilities for each node.

Step 1: Initialize the parameters in the static risk assessment graph and copy the components from the attack graph to the static risk assessment graph.

Step 2: Calculate the probabilities of occurrence and success for each threat node using prior knowledge.

Step 3: For each node:

- If it is an attack node, calculate its conditional probability table based on the probability of the attack occurring.
- If it is a resource node, calculate its conditional probability table based on the success probability of the attacks targeting it.

Step 4: Use the conditional probability tables and the prior probabilities of the initial attack nodes to calculate the prior probabilities of the resource nodes.

Step 5: Copy the calculated prior probabilities to the static risk assessment graph.

After obtaining the local conditional probability values of each state node, traverse the graph. All nodes (except the initial attack nodes) can derive their joint probability distributions based on prior knowledge and their parent nodes' influence. This distribution provides the probability of a state node transitioning to different risk states. Since attackers can sequentially gain various permissions for a host by exploiting vulnerabilities, changes in attacker permissions result in changes in the host's state. Therefore, the risk value calculation for a host requires summing up the probabilities of it transitioning to each risk state. To simplify the graph's structure, consider representing a particular vulnerability or permission as a resource node, with its value being either true or false to indicate whether the asset has been compromised.

This algorithm is generally used to assess potential risks in target networks that are not yet in use. Once the probabilistic graph model is constructed, the risk assessment results are fixed unless the prior knowledge is adjusted, giving each node a static risk value. However, security conditions and factors in operational systems constantly change over time. Therefore, dynamic factors must be considered for accurate risk assessment. In this context, the accuracy of prior-probability-based risk assessments decreases because reality does not always match prior knowledge. By incorporating real-time security incidents to update the attribute state nodes' probability distribution in the static risk assessment graph, security risks under dynamic conditions can be more accurately evaluated.

3.2. Dynamic Risk Analysis

The following steps outline how to derive a dynamic risk assessment probabilistic graph using both the static risk assessment probabilistic graph and real-time security incidents.

Input: Static risk assessment probabilistic graph $SAG = (S, A, E, R, T, P_1)$;

Output: Dynamic risk assessment probabilistic graph $DAG = (S, A, E, R, T, P_1, P_2)$, where P_2 is the set of posterior probabilities for each node.

Step 1: Initialize the parameters in the dynamic risk assessment probabilistic graph DAG. Copy all components from the static risk assessment graph SAG to the dynamic risk assessment graph DAG.

Step 2: Identify the resource nodes corresponding to a detected attack incident in the static risk assessment graph, selecting the nodes to be updated in the Bayesian network.

Step 3: For each selected resource node S_j in the static risk assessment graph, adjust its posterior probability based on its current detected state, such that $P(S_j = 1) = 1$.

Step 4: For each parent node $S_k \in \text{Par}(S_j)$ of the attribute node S_j , update its reachability probability using the conditional probability table, and copy the results to P_2 . Repeat this step until all parent nodes have been calculated.

Step 5: Remove S_k from the parent node set $\text{Par}(S_j)$ and treat it as a child node. Repeat Step 4 to update the state of its parent nodes.

Step 6: Continue updating the parent node set $\text{Par}(S_j)$ until the root parent node (initial attack node) is reached.

Step 7: Based on the posterior probability of the root node, calculate and update the posterior probabilities of nodes not in the same path as the update nodes. Update the static risk assessment attack graph accordingly.

Step 8: For each detected attack incident, repeat Steps 2–7, combining different attack events to achieve real-time assessment of network security risks.

The dynamic risk assessment method based on the Bayesian attack graph addresses the lack of consideration for the dynamic impact of ongoing attack incidents on attribute nodes in the graph. It dynamically updates the risk values of each state node and host based on intrusion detection system (IDS) information, enabling the timely prediction of attackers' targets and attack paths. This method aligns more closely with real-world network environments than static risk assessment methods, allowing security personnel to implement different defense strategies based on varying alerts. As the risk of nodes in the graph changes, the total risk also changes. Monitoring these changes helps security personnel keep track of overall network security trends in different scenarios.

3.3. Attack Paths and Security Assessment Indicators

When attackers attempt to breach a system, they navigate through various nodes to reach the final target node, resulting in multiple possible attack paths. To better predict which path the attacker will likely use, it is crucial to identify potential attack paths. For a Bayesian network based on a directed acyclic graph, we can use the Depth-First Search (DFS) algorithm. The basic steps are as follows:

Step 1: Initialize an empty path list to store all identified paths;

Step 2: Start from the initial node and add it to the current path;

Step 3: If the initial node matches the target node, add the current path to the path list, indicating a successful path discovery;

Step 4: If the initial node is not the target node, iterate through each neighboring node. If a neighboring node is not in the current path, recursively call the DFS algorithm, treating this neighbor as the new starting node while keeping the same target node and path list, but using a copy of the current path;

Step 5: After the recursive call returns, remove the starting node from the current path to explore other paths;

Step 6: Repeat Steps 4 and 5 until all possible paths have been traversed;

Step 7: Return the path list containing all paths between the starting and target nodes.

For instance, in Figure 3a, there are two attack paths from the initial attack node S_1 to node S_4 : $\{S_1, S_2, S_4\}$ and $\{S_1, S_3, S_4\}$. If the intrusion detection system detects that S_2 has been compromised, we can deduce that the attacker used the first attack path. In practice, Bayesian network models are often more complex than this illustration. To determine which attack path the attacker is most likely to use, or which path poses the highest risk to the assets, consider multiplying the probabilities of all compromised assets along the path to obtain the path reachability probability.

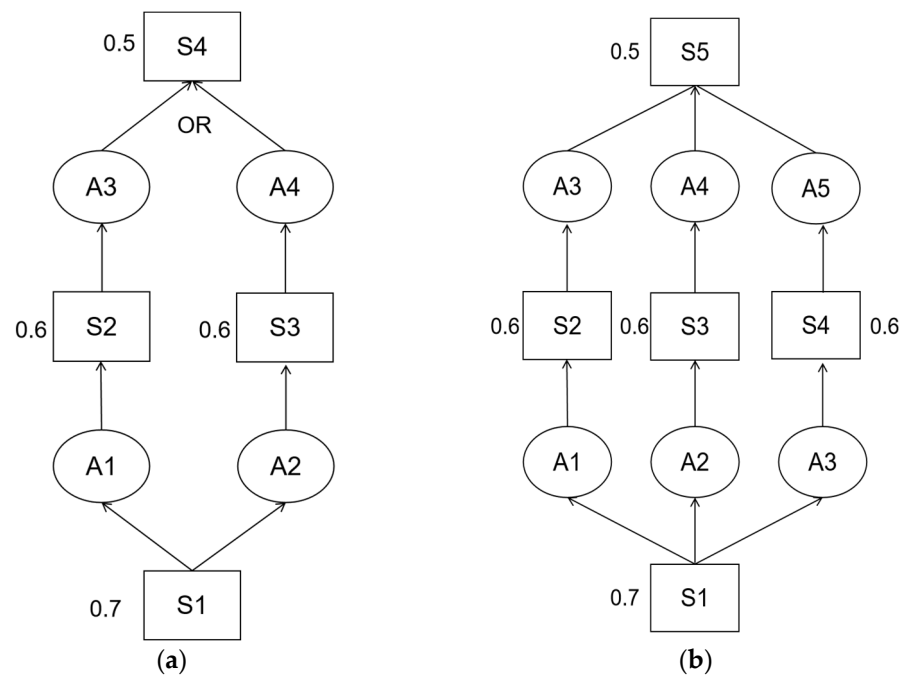


Figure 3. Comparison of two probability plots with different numbers of paths. (a) AG₁; (b) AG₂.

For any path, if the nodes on the path are denoted as S_j, then the reachability probability of this path is defined as follows:

$$P(path) = \prod P(S_j) \quad (6)$$

Given an initial and target node, the DFS algorithm can identify all possible paths between them. Using the above formula, the reachability probabilities of each path can be calculated, revealing which attack path is most likely to be exploited.

Due to the scale and complexity of real-world networks, their Bayesian networks can also be substantial. Comprehensive and targeted security assessment metrics are needed to evaluate the system's overall risk. Probabilistic graphs possess both graph structure and node probabilities, allowing for combined design metrics.

The Mean of Path Probability (MPP) is the arithmetic mean of all path probabilities in a probabilistic graph. The mean involves the entire probabilistic graph, and any path change may affect the average path probability. Thus, in some cases, the MPP can reflect changes in network security. The formula for calculating MPP is as follows:

$$MPP(AG) = \frac{\sum_{i=1}^n s(p_i)}{NP(AG)} \quad (7)$$

where

NP(AG): The number of paths in the probabilistic graph AG;

$s(p_i)$: Cumulative probability of all nodes in the attack path p_i .

Generally, the higher the MPP value, the lower the network security. The MPP indicator can capture the overall security level of the system. If the cumulative node probability for any path exceeds the MPP value, it indicates significant danger, and timely defensive strategies should be deployed.

However, the MPP does not always reflect the impact of path quantity on security. For example, Figure 3 shows that probabilistic graph AG₁ has two attack paths with a cumulative probability of 1.8, while AG₂ has three paths with a cumulative probability of 1.8. Evaluating these graphs using the MPP yields an average path probability of 1.8 for both. When each attack path has the same reachability probability, the graph with more

attack paths is riskier, which is not reflected in the MPP-based assessment. Thus, to account for the difference in the number of paths, the Normalized Mean of Path Probability (NMPP) is used:

$$NMPP(AG) = \frac{\sum_{i=1}^n s(p_i)}{\sqrt{MPP(AG)}} \quad (8)$$

Evaluating Figure 3 using NMPP:

$$NMPP(AG1) = \frac{3.6}{\sqrt{1.8}} = 2.68$$

$$NMPP(AG2) = \frac{5.4}{\sqrt{1.8}} = 4.02$$

The risk assessment results of probabilistic graphs AG1 and AG2 are 2.68 and 4.02, respectively. The results show that $NMPP(AG1) < NMPP(AG2)$, meaning that AG2 is riskier, which aligns with expectations.

4. Simulation and Results

Using the threat modeling method designed above, it is possible to quantitatively describe the new business scenarios of power systems. Moreover, the risk assessment methods, attack path analysis methods, and security assessment metrics designed above can quantify both local and overall risk states of the system, identify potential attack paths, and calculate the likelihood of these paths being exploited.

To compare the effectiveness of static risk assessment based on prior knowledge with dynamic risk assessment based on real-time security incidents, and to test the efficacy of the attack path analysis method and security metrics, a typical interactive scenario in new power system business is chosen. This scenario is modeled using a Bayesian network, and the conditional probability tables and exploitation probabilities for nodes are quantified according to the methods discussed above.

This study considers a typical small-scale local area network structure of a power system, as shown in Figure 4. In this simulated topology, the power system's LAN is divided into an internal network and an external network. Users can directly access the external network via a gateway, and also access the internal network through a relay server and video platform.

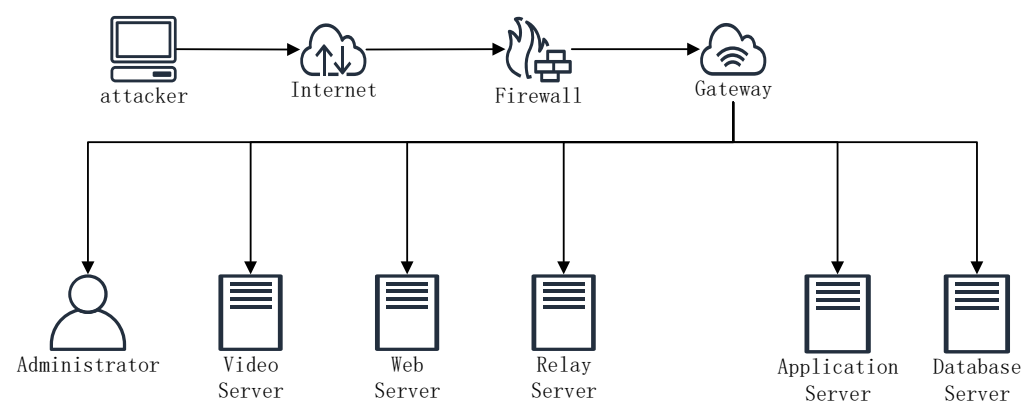


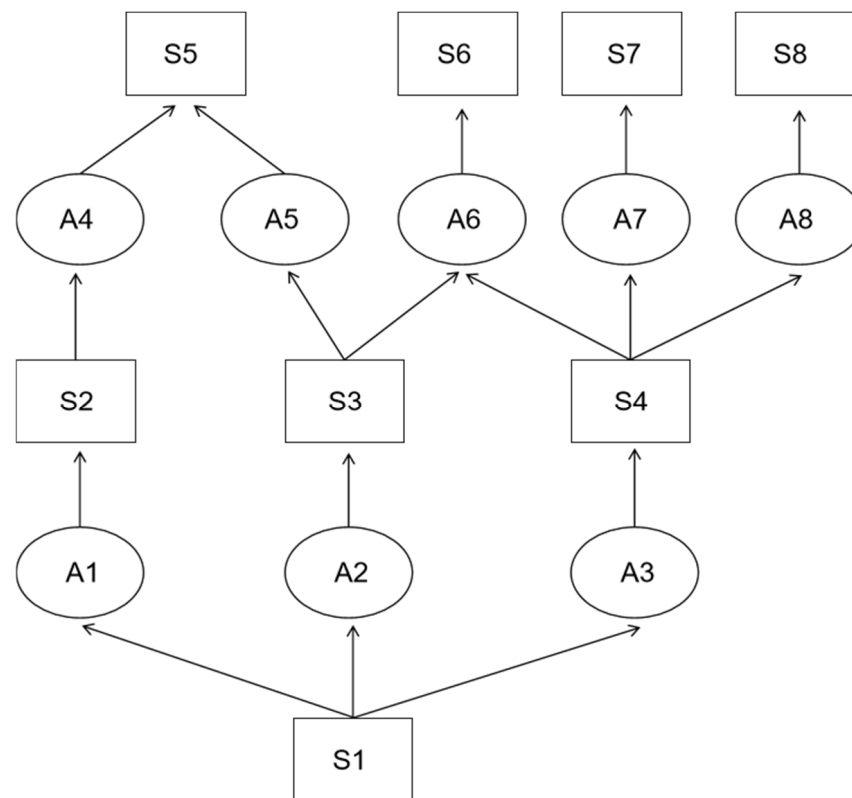
Figure 4. Network Environment Topology Diagram.

Nessus is used to scan host vulnerabilities in different network areas, and the detected vulnerability data are aggregated. The vulnerability information is shown in Table 3.

Furthermore, based on vulnerability information and network topology, a preliminary Bayesian attack graph can be constructed, as shown in Figure 5. In the figure, node relationships with multiple parent nodes are all OR.

Table 3. Vulnerability Information.

Hosts	Vulnerability Information	CVE-Number Vulnerability Number	Asset Number	Atomic Attack Number
Switch	Access Restriction Bypass	CVE-2015-8467	S2	A1
Relay Server	Buffer Cross-border Access	CVE-2012-4707	S3	A2
Video Server	Remote Code Execution	CVE-2015-1635	S4	A3
Administrator	Remote Code Execution	CVE-2004-0840	S5	A4
Administrator	IIS FTP Service Heap BOF	CVE-2010-3972	S5	A5
Database Server	Remote Code Execution	CVE-2013-4465	S6	A6
Video Server	Port Scanning	CVE-2015-1635	S7	A7
Application Server	Flooding Attack	CVE-2014-1446	S8	A8

**Figure 5.** Bayesian network model based on simulated experimental environment.

Based on a quantitative analysis of the vulnerabilities on each host in the system, the attacker's probability of launching an attack and exploiting a vulnerability successfully is calculated. Using the vulnerabilities and their exploitation relationships and probabilities, a Bayesian network model is constructed. Each attack node in the diagram corresponds to a vulnerability, and the attack success probability is the vulnerability exploitation success probability. To simplify the model, the node values are defined as 1 or 0 (logical true or false). If the attack succeeds, the resource node pointed to by the attack node is taken over by the attacker, and the corresponding random variable is set to 1, allowing the attacker to continue attacking further. If the attack fails and the asset remains unoccupied, the random variable is set to 0, preventing further attacks.

The conditional probability tables for each node can be derived by combining each attack node's success probability with the logical relationships between nodes. Thus, by initializing the initial attack node S_1 with an attack probability of 0.7, the prior probabilities of all resource nodes in the graph can be calculated using the static threat risk assessment algorithm based on prior knowledge. This will provide the prior probabilities for all resource nodes being in a risky state.

To assess vulnerabilities using CVSS metrics and calculate the exploitation and initiation probabilities, we refer to Equations (2) and (3) defined above. The calculation results are shown in Table 4. Since the accuracy of static risk assessment based on prior knowledge depends on the accuracy of the prior information, it does not always reflect the actual state of the system. When the intrusion detection system identifies an attack that successfully occurs, the corresponding resource node becomes an observed sample with a definite value rather than a random variable. As a result, the probabilities of other resource nodes falling into risky states will also change.

Table 4. Attack Initiation and Success Probabilities.

Attack Action	A1	A2	A3	A4	A5	A6	A7	A8
probability of launch	0.48	0.55	0.48	0.65	0.42	0.37	0.65	0.57
probability of success	0.69	0.55	0.41	0.76	0.61	0.54	0.95	0.69

However, static risk analysis methods cannot effectively adjust assessment results based on real-time attack detection. Therefore, by incorporating real-time attack data, the posterior probabilities of resource nodes in risky states can be calculated. This gives a probability that more accurately reflects the system's state under a specific attack event. For instance, if the relay server detects attack event A2, the posterior probabilities of other resource nodes in risky states can be computed using the dynamic threat risk assessment method under the assumption that A2 has occurred. Therefore, we assume that the attack represented by A2 is detected and calculate the probability based on this. The calculation results of prior and posterior probabilities are shown in Figure 6.

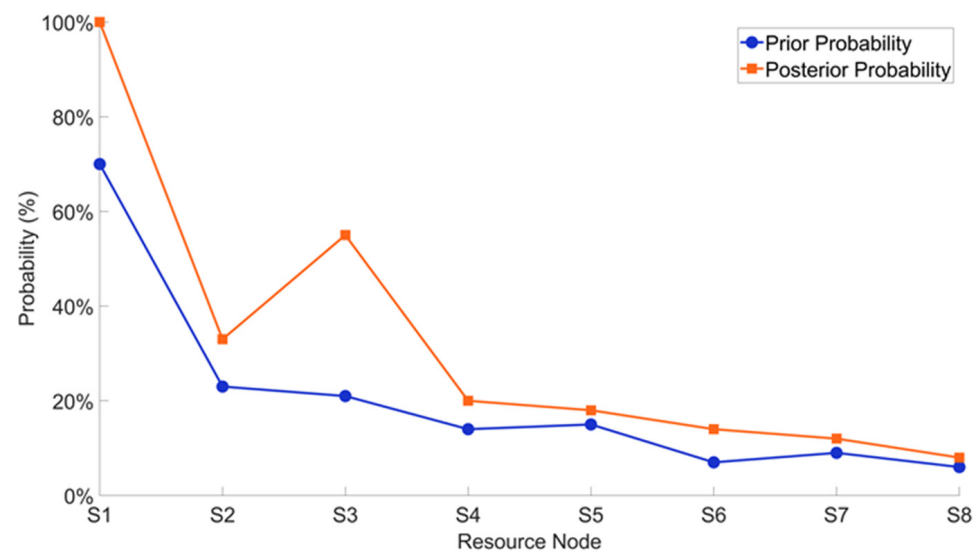


Figure 6. Prior and posterior probabilities of each node.

Using the relationships between nodes in the Bayesian network and the vulnerability status in the simulated environment, the prior probabilities of each attribute node are calculated using the static risk assessment algorithm. Suppose an intrusion detection system captures attack event A2 in the simulated environment. In that case, the dynamic risk assessment algorithm updates the probabilities of attribute nodes in the static attack graph, yielding posterior probabilities.

1. Attack Path Analysis

Based on the attack path analysis methods and security assessment metrics introduced earlier, security risk assessment results can be obtained under real-time attack scenarios. Six attack paths are identified in Figure 5: {S1, S2, S5}, {S1, S3, S5}, {S1, S3, S6}, {S1, S4, S6},

{S1, S4, S7}, and {S1, S4, S8}. These are labeled as Path 1–6, and their reachability probabilities are calculated using Equation (6). The calculation results are shown in Figure 7.

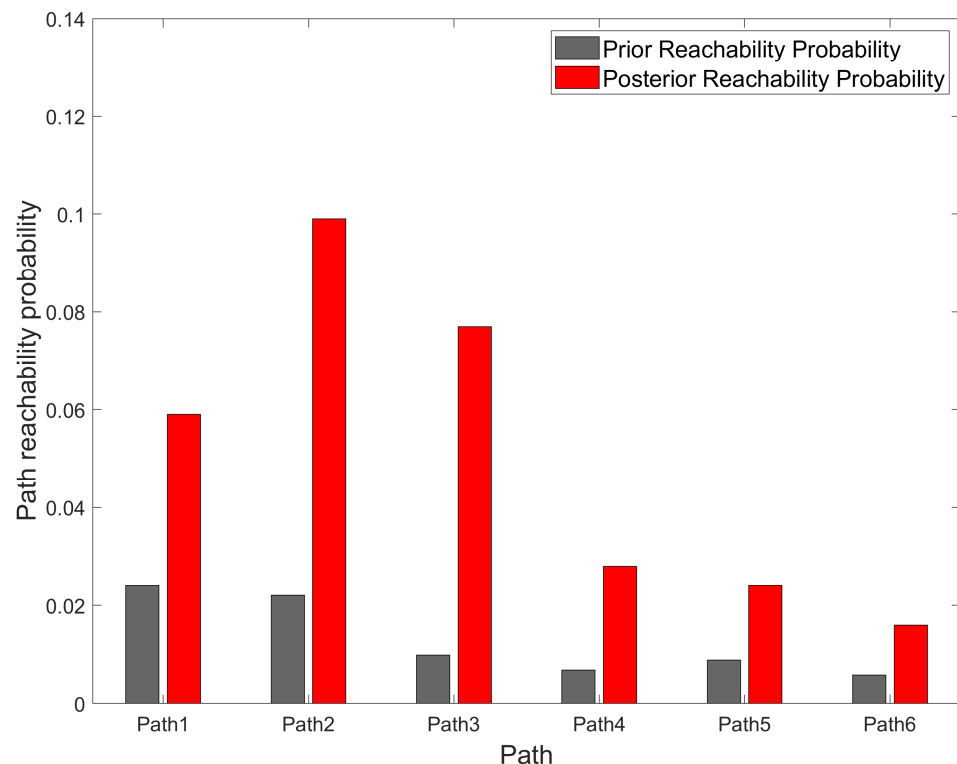


Figure 7. Path reachability probabilities.

The results indicate a key point. Regardless of whether prior or posterior probabilities are used, Path 2 has a relatively high reachability probability. This is because the nodes in Path 2 have higher vulnerability exploitation probabilities and valuable nodes, making the path highly attractive for attackers. Therefore, defensive strategies should focus on protecting assets along Path 2.

When attack event A2 is detected, the overall reachability probabilities of all attack paths increase, suggesting that every path is now riskier. Paths containing event A2, like Path 2 and Path 3, see the largest increase in reachability probabilities, indicating the attacker's intention. The data show that once the attacker's intent is known, the system's risk state changes. The posterior probabilities calculated using the dynamic risk assessment method more accurately reflect the system's actual risk at that moment.

2. Security Assessment Metrics

Bayesian networks in real-world scenarios often have large-scale and complex structures. To quickly visualize the system's overall security risk status, security assessment metrics specific to Bayesian networks are needed. The normalized mean of path probability (NMPP) is designed to capture the overall security risk by reflecting both node probabilities and path structures.

Before calculating the NMPP, the cumulative probabilities of all paths need to be calculated, which is the sum of the probability values of all resource nodes on the paths. Therefore, based on the previously mentioned environment, the prior cumulative probabilities and posterior cumulative probabilities of all paths are calculated separately, and the results are shown in Table 5.

Table 5. Path cumulative probability.

Path	Priori Cumulative Probability	Posterior Cumulative Probability
Path1	1.08	1.51
Path2	1.06	1.73
Path3	0.98	1.69
Path4	0.91	1.34
Path5	0.93	1.32
Path6	0.9	1.28

Based on the above calculation results and Equations (7) and (8). The calculation is as follows:

$$MPP_{pr} = \frac{\sum s(p_i)}{NP(AG)} = \frac{1.08 + 1.06 + 0.98 + 0.91 + 0.93 + 0.9}{6} = 0.978$$

$$MPP_{po} = \frac{\sum s(p_i)}{NP(AG)} = \frac{1.51 + 1.73 + 1.69 + 1.34 + 1.32 + 1.28}{6} = 1.478$$

Further,

$$NMPP_{pr} = \frac{\sum s(p_i)}{\sqrt{MPP_{pr}}} = \frac{1.08 + 1.06 + 0.98 + 0.91 + 0.93 + 0.9}{\sqrt{0.978}} = 5.93$$

$$NMPP_{po} = \frac{\sum s(p_i)}{\sqrt{MPP_{po}}} = \frac{1.51 + 1.73 + 1.69 + 1.34 + 1.32 + 1.28}{\sqrt{1.478}} = 7.29$$

The results show that $NMPP_{pr} < NMPP_{po}$, meaning that the NMPP calculated based on posterior probabilities is higher than that calculated based on prior probabilities. When a specific attack event is detected, the initial attack node is certainly 1 (attacker has initiated the attack). The occurrence of security event A2 raises the overall risk, reflected in the increase of the normalized mean of path probability.

The absolute value of NMPP indicates the overall risk level at a given moment. Higher NMPP values indicate higher security risk, calling for immediate defensive measures. By continuously monitoring the occurrence of security incidents, the system's risk level over time can be calculated to understand overall risk trends.

5. Conclusions

With modern networking and communication technologies widely integrated into monitoring and controlling power systems, vulnerabilities in communication networks expose highly interconnected power grids to new threats. Defenders must proactively identify network intrusions targeting power grids, determine potential attack paths, and deploy appropriate defense strategies. To address this issue, this paper proposes a Bayesian attack graph-based security assessment method for power systems.

Compared to existing studies, this paper quantifies Bayesian network node information by considering both the importance of assets and the cost of launching an attack to calculate the attacker's initiation probability. Additionally, it determines the probability of attack success based on the difficulty of exploiting vulnerabilities. Using these calculations, prior probabilities for each node are derived, reflecting the likelihood of assets being threatened based on past experiences.

Furthermore, this paper introduces a security assessment method that calculates the posterior probabilities of associated nodes based on real-time detected attack incidents. Posterior probabilities indicate the likelihood of threats to each node under specific conditions, and the system's security state changes accordingly with each detected attack event.

Additionally, an attack path analysis method and security assessment metrics are developed to assess the overall system risk status. Experimental results verify the effectiveness of the proposed risk analysis methods and security assessment metrics.

Author Contributions: Conceptualization, L.C. and T.Z.; methodology, L.C.; software, T.Z.; validation, L.C., Y.M. and Y.L.; formal analysis, Y.M.; investigation, C.W.; resources, C.H.; data curation, C.H.; writing—original draft preparation, T.Z.; writing—review and editing, L.C. and Z.L.; visualization, Y.M. and N.L.; supervision, C.W. and Z.L.; project administration, Y.L.; funding acquisition, N.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Science and Technology Project of State Grid Corporation of China. (Research on Flexible Secure Access and Unknown Attack Awareness Technology for New-type Business Terminals, 5108-202218280A-2-232-XG).

Data Availability Statement: All data are unavailable due to privacy restrictions.

Acknowledgments: We express our heartfelt gratitude to the reviewers and editors for their meticulous work.

Conflicts of Interest: Author Lu Chen, Tao Zhang, Yuanyuan Ma, Yong Li, Chen Wang, and Chuan He are employed by State Grid Smart Grid Research Institute Co., Ltd. Author Zhuo Lv and Nuannuan Li are employed by State Grid Henan Electric Power Company. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

References

1. Liu, C.; Stefanov, A.; Hong, J.; Panciatici, P. Intruders in the Grid. *IEEE Power Energy Mag.* **2012**, *10*, 58–66. [\[CrossRef\]](#)
2. Liu, F.; Zhang, S.; Ma, W.; Qu, J. Research on Attack Detection of Cyber Physical Systems Based on Improved Support Vector Machine. *Mathematics* **2022**, *10*, 2713. [\[CrossRef\]](#)
3. Abdelmalak, M.; Venkataramanan, V.; Macwan, R. A Survey of Cyber-Physical Power System Modeling Methods for Future Energy Systems. *IEEE Access* **2022**, *10*, 99875–99896. [\[CrossRef\]](#)
4. Zhang, Y.; Ni, M.; Sun, Y. Fully Distributed Economic Dispatch for Cyber-physical Power System with Time Delays and Channel Noises. *J. Mod. Power Syst. Clean Energy* **2022**, *10*, 1472–1481. [\[CrossRef\]](#)
5. Dong, Z.; Tian, M.; Ding, L. A Framework for Modeling and Structural Vulnerability Analysis of Spatial Cyber-Physical Power Systems from an Attack–Defense Perspective. *IEEE Syst. J.* **2021**, *15*, 1369–1380. [\[CrossRef\]](#)
6. Wang, W.; Yang, S.; Hu, F.; Stanley, H.E.; He, S.; Shi, M. An Approach for Cascading Effects within Critical Infrastructure Systems. *Phys. A Stat. Mech. Its Appl.* **2018**, *510*, 164–177. [\[CrossRef\]](#)
7. Lau, P.; Wang, L.; Liu, Z.; Wei, W.; Ten, C.W. A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability. *IEEE Trans. Power Syst.* **2021**, *36*, 5512–5524. [\[CrossRef\]](#)
8. Zhang, Y.; Wang, L.; Xiang, Y.; Ten, C. Power System Reliability Evaluation with SCADA Cybersecurity Considerations. *IEEE Trans. Smart Grid* **2015**, *6*, 1707–1721. [\[CrossRef\]](#)
9. Wu, H.R.; Qin, J.; Zheng, B.J. Anti-attack ability based on costs in complex networks. *Comput. Sci.* **2012**, *39*, 224–227.
10. Sun, F.; Pi, J.; Lv, J. Network security risk assessment system based on attack graph and Markov chain. *J. Phys. Conf. Ser.* **2017**, *910*, 012005. [\[CrossRef\]](#)
11. Hu, H.; Liu, Y.L.; Zhang, H.Q. Route prediction method for network intrusion using absorbing Markov chain. *J. Comput. Res. Dev.* **2018**, *55*, 831–845.
12. Xie, P.; Li, J.H.; Ou, X. Using bayesian networks for cyber security analysis. In Proceedings of the 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Chicago, IL, USA, 28 June–1 July 2010; pp. 211–220.
13. Poolsappasit, N.; Dewri, R.; Ray, I. Dynamic security risk management using bayesian attack graphs. *IEEE Trans. Dependable Secur. Comput.* **2012**, *9*, 61–74. [\[CrossRef\]](#)
14. Chen, X.J.; Fang, B.X.; Tan, Q.F. Inferring attack intent of malicious insider based on probabilistic attack graph model. *Chin. J. Comput.* **2014**, *37*, 62–72.
15. Gao, N.; Gao, L.; He, Y.Y. Dynamic security risk assessment model based on bayesian attack graph. *J. Sichuan Univ.* **2016**, *48*, 111–118.
16. Ma, C.G.; Wang, C.H.; Zhang, D.H. A dynamic network risk assessment model based on attacker’s inclination. *J. Comput. Res. Dev.* **2015**, *52*, 2056–2068.
17. Yazdi, M.; Zarei, E.; Adumene, S.; Abbassi, R.; Rahnamayiezekavat, P. Chapter Eleven—Uncertainty Modeling in Risk Assessment of Digitalized Process Systems. *Methods Assess Manag. Process Saf. Digit. Process Syst.* **2022**, *6*, 389–416.
18. Zhang, Y.; Ni, M. Security-Oriented Cyber-Physical Risk Assessment for Cyberattacks on Distribution System. *Appl. Sci.* **2023**, *13*, 11569. [\[CrossRef\]](#)
19. He, R.; Yang, S.; Deng, J.; Feng, T.; Lai, L.L.; Shahidehpour, M. Reliability Analyses of Wide-Area Protection System Considering Cyber-Physical System Constraints. *IEEE Trans. Smart Grid* **2021**, *12*, 3458–3467. [\[CrossRef\]](#)

20. Ten, C.W.; Liu, C.C.; Manimaran, G. Vulnerability assessment of cybersecurity for SCADA systems. *IEEE Trans Power Syst.* **2008**, *23*, 1836–1846. [[CrossRef](#)]
21. Zhang, Y.C.; Wang, L.F.; Sun, W.Q. Distributed intrusion detection system in a multi-layer network architecture of smart grid. *IEEE Trans Smart Grid* **2011**, *2*, 796–808. [[CrossRef](#)]
22. Qin, H.; Liu, D. Risk Assessment in Distribution Networks Considering Cyber Coupling. *Int. J. Electr. Power Energy Syst.* **2023**, *145*, 108650. [[CrossRef](#)]
23. Lagerström, R.; Ekstedt, M.; Franke, U. Can the Common Vulnerability Scoring System Be Trusted? A Bayesian Analysis. *IEEE Trans. Dependable Secur. Comput.* **2018**, *15*, 1002–1015.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.