information

MDPI

Article

Quantitative Model of Attacks on Distribution Automation Systems Based on CVSS and Attack Trees

Erxia Li [1], Chaoqun Kang [1], Deyu Huang [2,*], Modi Hu [2], Fangyuan Chang [1], Lianjie He [1] and Xiaoyong Li [2,*]

[1] China Electric Power Research Institute, Haidian District, Beijing 100192, China
[2] Key Laboratory of Trustworthy Distributed Computing and Service (Beijing University of Posts and Telecommunications), Ministry of Education, Haidian District, Beijing 100876, China
* Correspondence: huangdeyu@bupt.edu.cn (D.H.); lixiaoyong@bupt.edu.cn (X.L.)

Received: 27 May 2019; Accepted: 26 July 2019; Published: 29 July 2019

Abstract: This study focuses on the problem of attack quantification in distribution automation systems (DASs) and proposes a quantitative model of attacks based on the common vulnerability scoring system (CVSS) and attack trees (ATs) to conduct a quantitative and systematic evaluation of attacks on a DAS. In the DAS security architecture, AT nodes are traversed and used to represent the attack path. The CVSS is used to quantify the attack sequence, which is the leaf node in an AT. This paper proposes a method to calculate each attack path probability and find the maximum attack path probability in DASs based on attacker behavior. The AT model is suitable for DAS hierarchical features in architecture. The experimental results show that the proposed model can reduce the influence of subjective factors on attack quantification, improve the probability of predicting attacks on the DASs, generate attack paths, better identify attack characteristics, and determine the attack path and quantification probability. The quantitative results of the model's evaluation can find the most vulnerable component of a DAS and provide an important reference for developing targeted defensive measures in DASs.

Keywords: industrial control safety; attack quantification; common vulnerability scoring system; attack tree; distribution automation system

1. Introduction

1.1. Motivations

The expansion of the construction scale of distribution automation systems (DASs) and the increasing demand for their application have increased the risk of cyber and physical attacks on these systems. On 7 March 2019, Venezuela's power grid system experienced deliberate destruction [1]. Large-scale blackouts occurred in most parts of Venezuela, including its capital, Caracas, which experienced blackouts for more than 24 h. At one point, 20 of Venezuela's 23 states experienced blackouts, which seriously affected their infrastructure. In 2015, a sophisticated cyberattack targeted Ukraine's power grid and caused power outages over a wide area [2]. This highlights the importance of investment in securing power distribution grids against intruders [3]. Similarly, the overall safety of Chinese DASs must be improved, given the increasing demand for distribution network security [4]. At present, attack quantification in DASs at home and abroad remains in its infancy. DASs have high complexity and poor flexibility and lack a mature method for the quantitative evaluation of attacks on them [5–7]. Thus, ensuring DAS security has become a key challenge in the industry. To avoid disasters, defensive measures can be applied in advance through a reasonable quantitative evaluation of attacks and an evaluation of the probability of an attack on each part of a DAS [8]. Simultaneously,

these attack quantification results can also provide an important reference for security technicians to implement the DAS defense system.

Quantification of the probability of an attack on a DAS directly affects the in-depth analysis of the system's security. Wang et al. [9] proposed a multilevel analysis and modeling method for a power system's communication network. Their case study showed that this method can be used to evaluate the static and dynamic relationships among power networks. Kateb et al. [10] developed an optimal structure tree method for risk assessment in a wide-area power system that can minimize the spread of network attacks. The authors in [9,10] provided a well-optimized evaluation of a specific power network. However, these evaluation neither reflected the attacker's behavior in terms of quantification of the probability of an attack nor provided suggestions for the protection of specific parts of the power system. The authors in [11] and the authors in [12] presented an attack assessment framework based on Bayes attributes—a stochastic game model and a fast modeling method for input data, respectively—which included network connection relationship and vulnerability information. However, the proposed methods were found to be inefficient when applied in DASs due to DAS architecture complexity and expansibility, and they could not generate attack path. The authors in [13] proposed a method for modeling network attacks with a multilevel-layered attack tree (MLL-AT), presented a description language based on the MLL-AT for attacks, and quantified the leaf nodes. This attack tree (AT) was found to be able to accurately model the attacks, especially multilevel network attacks, and can be used to assess system risks. However, the research is mainly based on cyberattacks, and there is no physical attacks involved. Besides, this method lacks a complete attack process identification method, and its ability to analyze attack paths is insufficient.

1.2. Main Contributions

To summarize, although a number of studies have developed measures to quantify system risks or attacks, they insufficiently describe attack behavior or attack paths. These measures are affected by subjective factors, which are unsuitable for attack quantification of distribution automation systems. To solve these problems, we propose a modeling method for quantifying attacks on DASs based on common vulnerability scoring system (CVSS) and ATs form the perspective of the attacker's behavior. The proposed node attack probability quantification algorithm combined with the CVSS has favorable expansibility. This algorithm can improve the probability of predicting attacks on DASs, generate attack paths, and discover the latest protection component.

To our knowledge, this study is the first to use the AT to quantify the probability of attacks in DASs, which is systematic and quantitative evaluation of attacks in DASs. The main contributions are as follows.

- First, a DAS security architecture is developed on the basis of the functional characteristics and security protection requirements of DASs. This architecture provides an intuitive view of the security components of a DAS, which can help system designers have a clear understanding of the path to possible cyber-attacks and physical-attacks.
- Second, a DAS attack quantification model was established by forming a set of complete attack processes and paths based on attacker behavior, which can help DAS security practitioners to find the system components that should be defended, helping penetration testers to deploy targeted and focused attacks.
- Third, a quantification algorithm for attack probability based on an AT and the CVSS was proposed. This algorithm reduces the influence of the subjective factors in the process for quantifying attacks in traditional approaches and improves the accuracy of attack prediction. The efficacy of the model was evaluated by introducing the environmental characteristics of the DAS.

The experimental results show that the proposed model can predict the risk of attack that the DAS faces. The results of the model's evaluation verify feasibility, effectiveness of the proposed scheme and provide an important reference for the development of targeted defensive measures for DASs.

The rest of this paper is structured as follows: Section 2 gives a detailed design of the DAS security architecture. The quantitative model of attacks on DAS based on CVSS and ATs is described in Section 3. The experimental results are presented in Section 4. Finally, Section 5 concludes the paper.

2. Design of the DAS Security Architecture

DASs have the characteristics of a large number of terminals, high complexity architecture, poor flexibility, and require strict protection against both network attacks and physical attacks [14]. A DAS security architecture was developed on the basis of the functional characteristics and security protection requirements of DASs. It is shown in Figure 1.

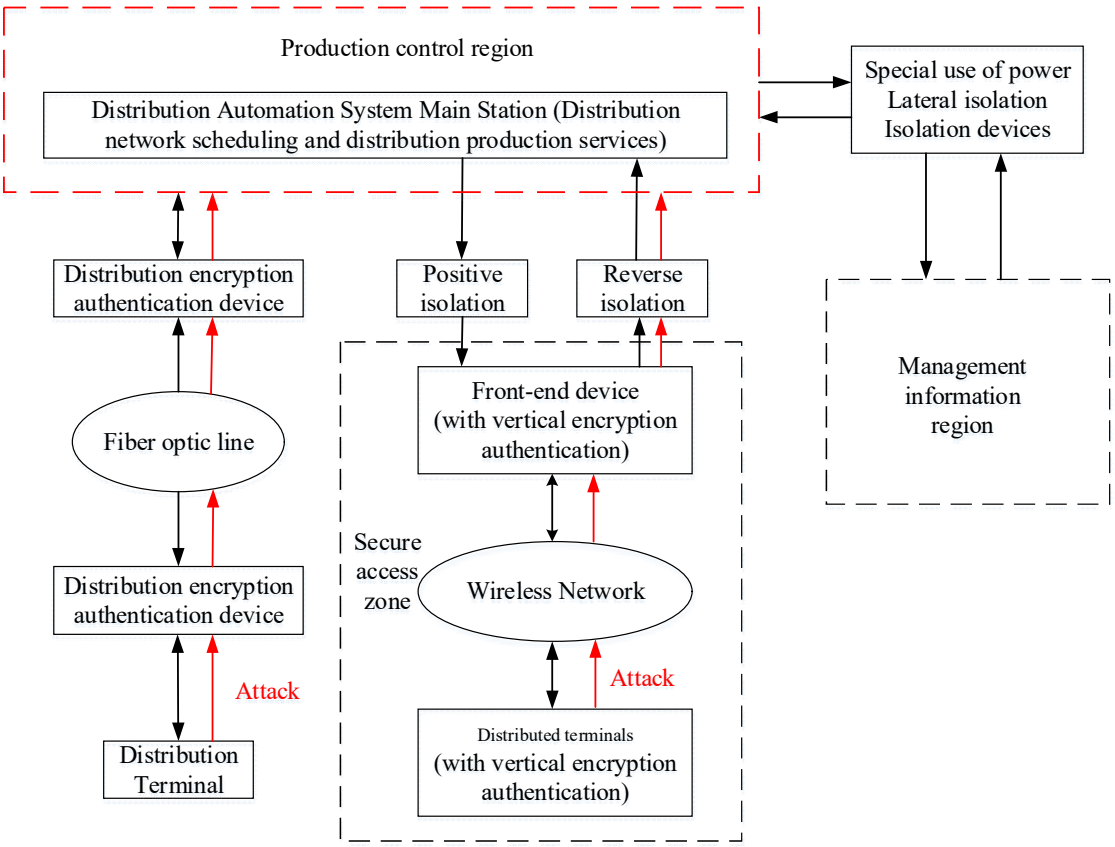

Figure 1. Distribution automation system (DAS) security architecture.

(1) The production control region directly manages the distribution automation system's main station and controls the automatic power distribution scheduling of the entire distribution network. It is at the core of the DAS's distribution scheduling and production services. It includes the main station's server, the main station's monitoring computing station, the main station's transport unit controller, and other equipment, which are vulnerable to phishing, distributed denial-of-service attacks, and physical attacks [15].

(2) The communication mode of the application part of the management information region is based mainly on public network communication. It is connected to the production control region by an isolation device to realize a large amount of data storage and thus is very sensitive to Web data security.

(3) The secure access zone includes wireless network, some acquisition servers, and the front-end device that transmits commands and collects terminal data so that the DAS can realize intelligent power distribution and optimized operation. As the link between the core of the distribution network and the terminal information exchange, this zone faces many security risks. An attacker can use the terminal as a springboard to invade or attack through the wireless network.

(4) At the furthermost edge of the DAS is the power distribution terminal. It can communicate with the main station through an optical fiber. Although this part of the equipment is a great distance away from the core equipment for power distribution, it is the smallest unit and supplies power to the distribution automation system. It is the point of the system that is most vulnerable to attacks.

3. DAS Attack Quantification Algorithm

In order to face the different security attacks that can occur in the DAS security architecture, an attack probability quantification model based on an AT for the DAS framework is proposed. Each leaf node of the AT represents an attack on a certain component of the DAS security architecture. The maximum probability of each attack path in ATs will be calculated on the basis of the CVSS in terms of three measurement factors— base, time, and environment.

3.1. DAS AT Model

The AT was first proposed by Schneier [16]. In the structure of an AT, the root node represents the target of the attack [17]. The characteristics of system security are described on the basis of the AT. These descriptions redefine the data on attacks by identifying whether the DAS security or survival criteria are satisfied, and the data are regarded as the root nodes of the tree. In Figure 2, a node represents the means of implementing an attack, and the relationship among the nodes may be the logical OR, that is, the attack target can be reached when one of the two nodes E1 and E2 satisfies the attack conditions; AND, that is, the attack target can be reached when nodes E1 and E2 satisfy the attack conditions simultaneously; or Order AND, that is, when the attack target is reached after nodes E1 and E2 satisfy the attack conditions [18]. The AT has the advantages of simple structure, easy to understand presentation method, and easy to focus the analysis process on measurable targets. It can be combined with the obvious features of DAS in terms of architecture and simplify the DASs of system security features.

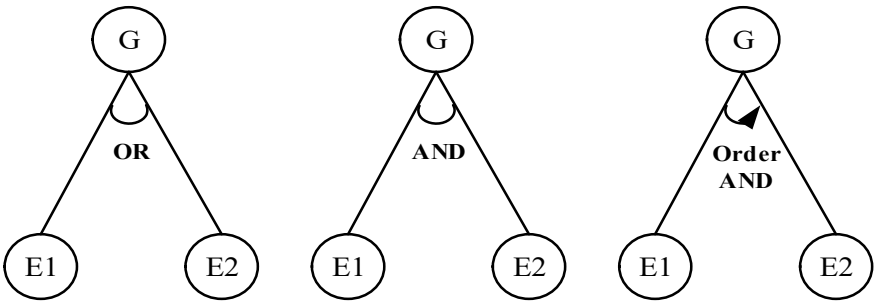

Figure 2. Node representations in the attack tree (AT).

The DAS AT model must consider the environment and the DAS security architecture. Figure 3 shows the main stages of the DAS AT model. The nodes of all leaves will first be quantified when the ATs are established. Then, the probability of a successful attack in all paths of the system will be calculated by modeling the DAS AT. The attack path sequence is obtained through calculation, and the path with the maximum attack probability is the optimal attack path.

The use of software vulnerabilities is a well-known way to attack a network. Our attack probability quantification algorithm is based on the CVSS. The attack probability value of the Common Vulnerabilities and Exposures (CVE) vulnerabilities at each node of the DAS is calculated using the CVSS method. Furthermore, combined with the method of attacking the tree, each path the attack probability of the DAS is calculated to evaluate the probability of each attack.

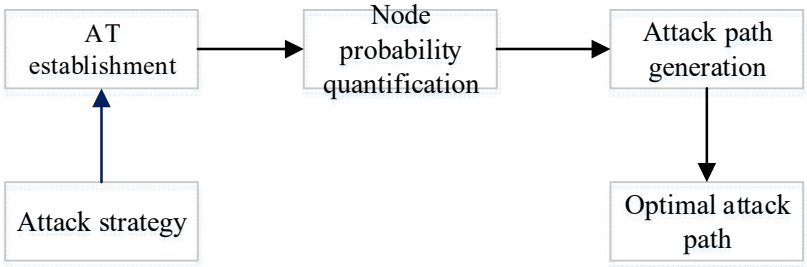

Figure 3. The main stages of the DAS AT Model.

3.2. CVSS

The CVSS is a standard for calculating the risk level of each CVE vulnerability. It was developed by the National Infrastructure American Council and is maintained by the Forum of Incident Response and Security Teams [19]. Manufacturers can adopt this system for free. On the basis of the CVSS, we can score a system's weaknesses and determine which weaknesses have priority for repair. The CVSS provides an open framework for evaluating the characteristics and impact of system vulnerabilities for information security industry–related practitioners. The CVSS quantifies CVE vulnerabilities using scores (0–10) of severity, and strict attack indexes can be formulated, including attack vector, attack complexity, authentication, availability, integrity, and confidentiality indexes [20].

As shown in Figure 4, the CVSS consists of three basic score indicators, namely the base score, the temporal score, and the environmental score. The base score includes exploitability metrics and impact metrics, which have their own calculation formulas. The temporal and environmental scores can be expanded. Moreover, a vector string and a CVSS score, which represent the calculation process and the result, respectively, are generated.

The CVSS is supported by the National Vulnerability Database (NVD) of the United States. All CVE vulnerabilities in the NVD contain the basic value of the CVSS [21]. The quantification of the DAS attack probability is closely related to the evaluation indexes of vulnerabilities for all parts of a DAS and plays an important auxiliary role in the quantification of an attack process in the DAS. Thus, the probability of attack that the DAS faces is quantified on the basis of the CVSS.

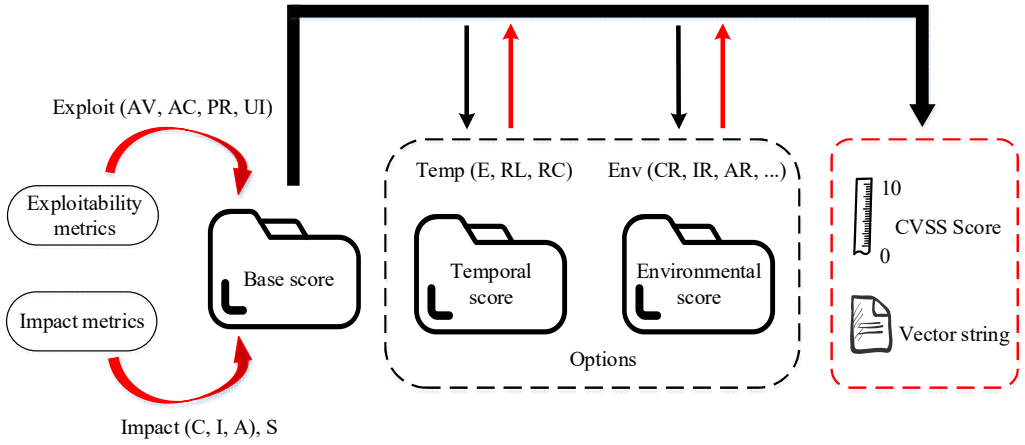

Figure 4. Score calculation in the common vulnerability scoring system (CVSS).

Table 1 lists the relevant variables for calculating the CVSS base score [22]. In accordance with these variables, the base score represents the inherent characteristics of the vulnerability itself and the possible impact of these characteristics. The scoring situation can determine the attack probability that the vulnerability represents.

Table 1. Base score calculation-related metrics.

Relevant Metrics	Possible Metric Values	Quantified Scores
Attack vector (AV)	Network (N)/Adjacent (A)/Local (L)/Physical (P)	0.85/0.62/0.55/0.2
Attack complexity (AC)	Low (L)/High (H)	0.77/0.44
Privilege required (PR)	Non (N)/Low (L)/High (H)	0.85/0.62/0.27
User interaction (UI)	Non (N)/Requirement (R)	0.85/0.62
Scope of influence (S)	Unchanged (U)/Changed (C)	Depends on ESS, ISC
Confidentiality (C)	Non (N)/Low (L)/High (H)	0/0.22/0.56
Integrity (I)	Non (N)/Low (L)/High (H)	0/0.22/0.56
Availability (A)	Non (N)/Low (L)/High (H)	0/0.22/0.56

For example, the scoring rubric for Attack Vector (AV) is divided into four possible metric methods. Figure 5 shows the division of measurement methods [22]. The score increases in the direction of the arrow in the figure. For example, the metrics of Network (N) and Adjacent (A) are the vulnerable components via the network stack, and the metrics of Local (L) and Physical (P) require physical access to the target. Network (N) can be exploited from across a routed network, which makes it easier to implement network attacks, so the measurement value is higher. However, the metric of Adjacent (A) is only exploitable across a limited logical or physical network distance.

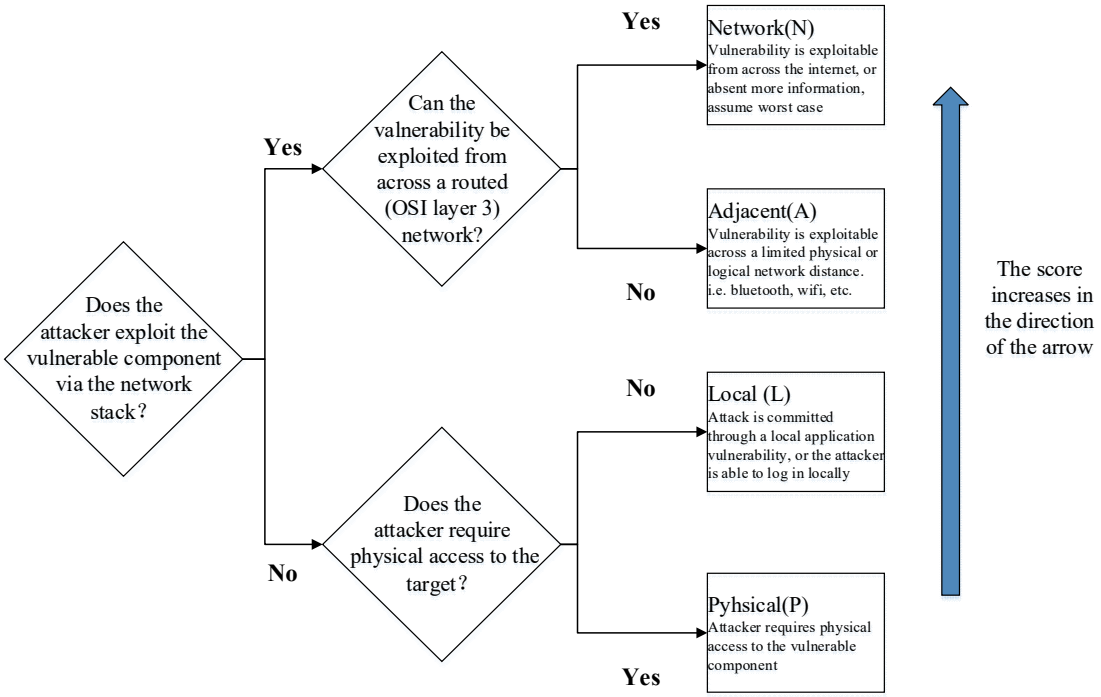

Figure 5. The scoring rubric for the Attack Vector metric.

3.3. Attack Probability Quantification Algorithm Based on the AT

To quantify the attack probability of the entire DAS, we must first determine the attack probability of each key module (leaf node) in the DAS. Second, all of the potential attack paths in the AT need to be traversed to count the probability of each path and determine the most probable attack path. On the basis of the CVSS characteristics, the vulnerability attack probability P_{attack} of a leaf node is defined as

$$\frac{Base\ Score + Temp\ Score + Envi\ Score}{10.0 * (1 + n)}, \tag{1}$$

where *Temp Score* and *Envi Score* denote the temporal and environmental scores, respectively, which can be expanded by a vulnerability to a user's environment. However, base score is a mandatory option, but scoring the Temporal and Environmental metrics is optional. n denotes the number of temporal scores and environmental scores. The *Base Score* consists of the exploitability sub score (ESS) and the impact sub score (ISC). ESS and ISC are related to the scope of influence in the factors (scope). The Base Score value is calculated using Algorithm 1 [22].

Algorithm 1. Calculate the value of the Base Score.

Input: ESS (Exploitability Sub Score); ISC (Impact Sub Score)
Output: Base Score
(1) **procedure**: *Base Score*, *Roundup*()
(2) **If** ISC <= 0 **then**
(3) *Base Score* = 0
(4) **else if** ScopeUnchanged **then**
(5) *Base Score* = *Roundup* (*Minimum* [(ESS + ISC), 10])
(6) **else**
(7) *Base Score* = *Roundup* (*Minimum* [1.08 × (ESS + ISC), 10])
(8) **end if**
(9) **end procedure**

The ISC, which is determined by the confidentiality, integrity, and availability indexes, is calculated using Algorithm 2.

Algorithm 2. Calculate the value of impact sub score (ISC).

Input: *ImpactConf*; *ImpactInteg*; ImpactAvail
Output: ISC
(1) **procedure**: ISC
(2) ISCtmp = 1 − [(1 − ImpactConf) × (1 − ImpactInteg) × (1 − ImpactAvail)]
(3) **if** ScopeUnchanged **then**
(4) ISC = 6.42 × *ISCtmp*
(5) **else if** Scopechanged **then**
(6) ISC = 7.52 × [*ISCtmp* − 0.029] − 3.25 × [*ISCtmp* − 0.02]^{15}
(7) **end if**
(8) **end procedure**

The relationships between ESS and Attack Vector (AV), ESS and Attack Complexity (AC), ESS and Privileges Required (PR), and ESS and user interaction (UI) are expressed as

$$ESS = 8.22 \times AV \times AC \times PR \times UI. \quad (2)$$

After calculating the attack probability of a single node, the formula for calculating the probability of a successful attack at the parent node is based on two nodes, namely the AND and OR nodes.

(1) For the AND or Order AND node, the attack probability of the current parent node G is the product of the attack probability at the child nodes.

$$P_{\text{attack}}(G) = \prod_{i=1}^{n} P_{\text{attack}}(Gi) \quad (3)$$

(2) For the OR node, the attack probability of the parent node G is the maximum attack probability of the child nodes.

$$P_{\text{attack}}(G) = \max\{P(G1), P(G2), \ldots, P(Gn)\} \quad (4)$$

A traversal from a leaf node to a root node represents a possible attack path within the DAS. Based on the calculation of the attack probability at the AND and OR nodes, the target node that attacks a certain attack path $S_j = \{G_i | \, i = 1, 2, \ldots, n\}$ is set as G, and the probability of a successful attack is

$$P_{\text{attack}}\left(S_j\right) = \prod_{i=1}^{n} P_{\text{attack}}(Gi) \tag{5}$$

When $P_{\text{attack}}\left(S_j\right)$ is high, both the probability of a successful attack and the risk factor of the system will also be high. Thus, a defense can be firmly mounted. The maximum attack probability of the entire system can be expressed as

$$P_{\text{attackmax}}(S) = \max\left\{P(S_1), P(S_2), \ldots, P\left(S_j\right)\right\} \tag{6}$$

4. Experimental Evaluation

To verify the feasibility and effectiveness of the attack probability quantification algorithm, an attacker model was established through the quantification algorithm, and an experimental environment was built. The comparison was performed using a quantification algorithm from the literature.

4.1. Construction of the Experimental Environment

An attacker's abilities, state, and DAS-related information should be determined before quantitative modeling. These data are used as a bridge between the attacker behavior and a system attack probability analysis. An attacker can launch an attack from anywhere inside or outside the system. On the basis of an attacker's worst possible attack behavior [23,24], we adopt the following assumptions: (1) attackers are knowledgeable about the DAS and have up-to-date DAS vulnerability information, (2) attackers can deliberately and effectively attack using social engineering, (3) the minimum expected attack income gains are obtained before an attacker attacks, and (4) effective attacks frequently have a few atomic attack steps.

In this group of experiments, the AT is built to destroy the safe operation of the DAS. The DAS AT and attack paths were established as shown in Figure 6 on the basis of attackers' behavior and all the vulnerability and possible attacks of various components of the actual system in Section 2. Each leaf node of the AT represents an attack on a certain component of the DAS security architecture. After the leaf node attack probability has been calculated, the leaf node that is set back from a leaf node traversal to the root node generates a complete attack path. A root node indicates that the attack has reached G. On the basis of the different types of attacks, intrusions into the DAS can be divided into G1 (a network attack through the distribution terminals and the information management region) and G2 (an attack through the physical equipment in the production control region). The system is captured and loss is caused when any attack on G1 and G2 occurs.

Table 2 presents the definitions for all nodes in the DAS AT shown in Figure 5 together with the DAS security architecture. For example, in the attack path E5 > H3 > H1 > G1, H3 denotes an attack after acquiring a puppet machine and is an OR node, which requires one of the leaf nodes to be attacked (e.g., E2, E3, E4, or E5). After a remote network attack, E5 implants a virus-controlled puppet (H3), thereby making it reach G1 through an Internet attack (H1) and invade G to achieve a complete attack. Path E6 > H2 > G1 > G indicates that leaf node E6 reaches G1 through H2 (an internal local area network (LAN)) to crack the internal wireless network password and obtain traffic information, thus breaking into the DAS to achieve intrusion.

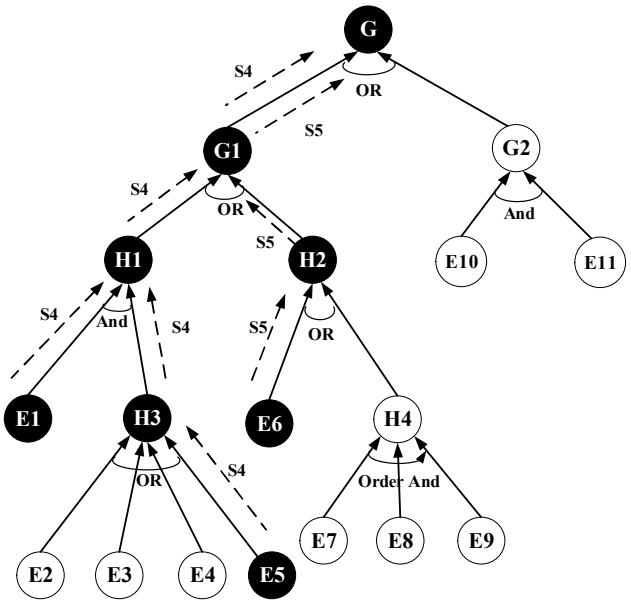

Figure 6. The DAS AT and attack path.

Table 2. Definitions for all nodes in the DAS AT.

Nodes	Definitions
G	Damaging/intruding into the DAS, endangering security
G1	Reaching G through a network attack
G2	Reaching G through an attack on physical equipment
H1	Reaching G1 through an Internet attack
H2	Reaching G1 through internal and related business network attacks
H3	Attack after acquiring a puppet machine
H4	Acquiring sensitive information from the internal database
E1	Implanting a Trojan horse into the control server
E2	Obtaining server data through phishing mail/web pages
E3	Intruding through a distributed denial-of-service attack
E4	Obtaining data by invading a web service of the DAS on the Internet
E5	Intruding through remote network vulnerabilities
E6	Cracking an internal wireless network password to obtain traffic information
E7	Scanning internal network port, service, and other asset information
E8	Acquiring root access to the database
E9	Attempting remote code execution through SMB vulnerabilities
E10	Entering into the distribution automation system through social engineering
E11	Breaking the BIOS through a u-disk to bypass a password requirement

4.2. Analysis of the Experimental Results

The CVE vulnerability numbers were established on the basis of the attack characteristics of each leaf node $\{E_i | \, i = 1, 2, \ldots, n\}$ and a DAS enterprise vulnerability evaluation in order to reflect the generality of the system components in the experiment involving a DAS while avoiding an attack-oriented experiment involving a hacker. System component vulnerabilities are not fully exploitable vulnerabilities in current DASs but rather represent vulnerabilities with different vendor components of the same type. For example, we choose the vulnerability number CVE-2018-0247 that is same type of vulnerability of Cisco Wireless LAN Controller for E6. The vulnerability attack probability of each leaf node was calculated by combining Equations (2) and (3) with Algorithms 1 and 2. Table 3 summarizes the DAS components and the vector string and P_{attack} results.

For example, E1 denotes the embedding of a Trojan horse into the control server. This activity occurs in the distribution encryption authentication device. The corresponding vulnerability number is CVE-2017-5873, and its vector string is AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H. AV is local (0.55), AC is low (0.77), PR is high (0.27), UI is unnecessary (0.85), the scope of influence (S) is unchanged, confidentiality (C) is high (0.56), integrity (I) is high (0.56), and availability (A) is high (0.56). Based on Algorithm 2, in the case of *ScopeUnchanged*, *ISCtmp* is correlated with AC, AV, and PR; that is, $1 - (1 - 0.55) \times (1 - 0.77) \times (1 - 0.27) = 0.924445$, and the ISC is $6.42 \times ISCtmp = 5.9$. Based on Equation (3), the ESS is $8.22 \times AV \times AC \times PR \times UI = 0.8$. Furthermore, in combination with Algorithm 1, the *Base Score* is 6.7. Based on Equation (2), P_{attack} is 0.67. Table 3 shows that the probability of a successful attack on the distributed encryption authentication device at this node using its vulnerability number (CVE-2017-1287) is more than 60%.

As shown in Table 4, the AT contains seven attack paths, namely S1 = (E1, E2), S2 = (E1, E3), S3 = (E1, E4), S4 = (E1, E5), S5 = (E6), S6 = (E7, E8, E9), and S7 = (E10, E11).

Table 3. Results on the attack probability of the DAS nodes.

Leaf Nodes	Vulnerability No.	DAS Components	Vector String	P_{attack}
Figure 6E1	CVE-2017-1287	Distributed encryption authentication device	AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N	0.67
E2	CVE-2017-5873	Management information region terminal	AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H	0.54
E3	CVE-2018-1137	Front-end device	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H	0.81
E4	CVE-2017-5873	Management information region terminals	AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N	0.48
E5	CVE-2018-9935	Distributed terminal	AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H	0.88
E6	CVE-2018-0247	Wireless network in the security access region	AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:N	0.47
E7	CVE-2015-6314	Production control region server	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	0.98
E8	CVE-2015-596	Acquisition server in the security access region	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	0.62
E9	CVE-2018-3269	Production control region server	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L	0.53
E10	CVE-2017-2839	Monitoring computing station in the main station	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	0.59
E11	CVE-2009-0243	Transport unit controller in the main station	AV:L/AC:L/UI:N/C:C/I:C/A:C	0.72

On the basis of the leaf node attack probability (Table 3), the probability on each attack path can be calculated by combining Equations (4)–(7). Each serial number represents an attack path sequence. Table 4 displays the results of the calculation of the attack path sequence probabilities. S6 represents E7, E8, and E9. In Figure 2, the node is Order AND. Based on Equation (4), $P_{attack}(H4)$ is the product of E7, E8, and E9; that is, $0.98 \times 0.62 \times 0.53 = 0.322$. Based on Equation (6), the maximum probability of $P_{attack}(\mathrm{G})$ is the attack probability of S4; that is, 0.5896. These results show that the maximum probability of a successful attack on the existing DAS is greater than 50%.

Table 4. Results of the calculation of the attack path probability.

Serial No.	Attack Paths	Attack Probability
S1	E1, E2, G1, G	0.3618
S2	E1, E3, G1, G	0.5427
S3	E1, E4, G1, G	0.3216
S4	E1, E5, G1, G	0.5896
S5	E6, G1, G	0.47
S6	E7, E8, E9, G1, G	0.322
S7	E10, E11, G2, G	0.4248

The Bayes method [11] was compared with the proposed attack probability quantification method to verify the latter's accuracy. The Bayes method aims to quantitatively evaluate the vulnerability of computer networks using a Bayes attribute attack graph and the CVSS. Figure 7 shows the results of the comparison. The two methods for evaluating attack sequence probability exhibit different performance with respect to highlighting risky paths. Figure 7 shows that the proposed AT model obtains a higher attack probability than the Bayes method when evaluating paths S2 and S4. In an actual DAS architecture displayed in Figure 1, the attack probability on paths S2 and S4 is the highest, which represents E1 Distributed encryption, E3 Front-end device, and E5 Distributed terminal in DASs. The probability result of the attack sequences obtained by the two methods are slightly different, and both S2 and S4 are the attack paths with the highest risk probability, which also verifies the reliability and validity of the proposed method. On the other hand, the proposed AT model probability is higher than the Bayes method probability 4.02%—6.11% in conditions S2 and S4. From Figure 7, the proposed method probability of attack is higher than the Bayes method, and the experimental result is conducive to security practitioner to pay more attention to the protection of dangerous parts of DASs.

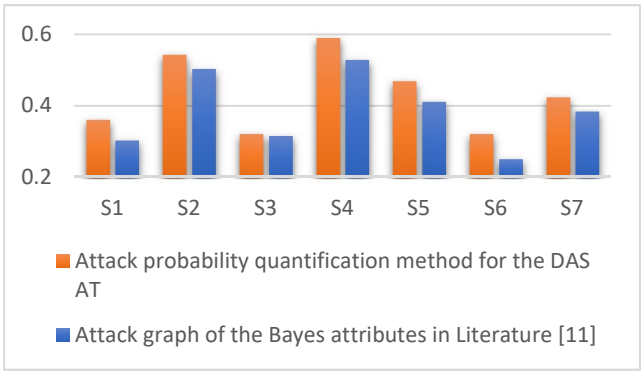

Figure 7. Comparison of the attack path probability for the DAS cases.

Due to the adoption of AT to construct DAS security architecture and attack paths, the advantage of this method is that it has more accurate probability calculation ability for network attacks and also more suitable for DASs with complex hierarchical network structure. The DAS attack quantification model is established by forming a set of complete attack processes and paths based on attacker behavior, which can help DAS security practitioners to find the system components that should be defended and help penetration testers to deploy targeted and focused attacks.

Compared with the Bayes method, the AT has the advantages of simple structure, and it is easy to focus the analysis process on measurable targets. It can be combined with the obvious features of DAS in terms of architecture and simplify the DASs of system security features. The logical "OR" and the logical "AND" characteristics of AT are very beneficial to construct such a complex DAS. At the same time, combining the characteristics of AT and DASs based on attacker behavior generated all the attack paths. Taken together, the proposed method is more effective than the Bayes method.

This finding reflects that an attack will succeed if the attackers have an abundance of information on the system. When combined with the actual security situation of the DAS, the experimental result predicts the danger of these paths and helps us to determine the components that must be defended considering that these components provide the DAS with effective defense solutions. Therefore, the proposed method is more effective than the Bayes method.

Figure 8 shows the proportions of all attack paths for the DAS. The DAS attack risks of each attack path in the system are emphasized, and the most dangerous part of the system is identified. Table 4 and Figure 8 show that the most profitable attack sequences for attackers are S2 and S4 in this experiment, and the corresponding attack methods are distributed denial-of-service attacks and website intrusions. Therefore, the DAS security practitioners should spend more time focusing on defending against these

associated attacks and system vulnerabilities. For example, defense measures for the network traffic at the web end and the main station's server could be applied.

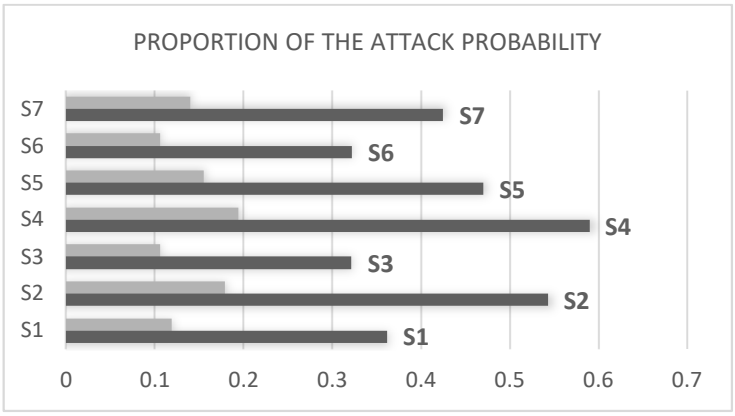

Figure 8. Proportions of the attack path probability for the DAS cases.

The evaluation methods [9–13] are based on a vulnerability analysis of traditional computer nodes and cannot quantify the attack probability of DASs. The proposed attack probability quantification algorithm and attack path calculation method can describe the vulnerability of the target system component of the DAS. To improve the accuracy of the quantification based on Algorithms 1 and 2, a set of complete attack processes and paths was constructed. The attack path with the maximum probability (Table 4) was determined to help security personnel find the attack path and DAS components with the most defense.

5. Conclusions

DASs are important to national infrastructures, which have experienced increasingly serious threats to information security. The safe and reliable operation of a DAS is directly related to the national economy and people's livelihood. In this study, a quantitative and systematic evaluation of DAS attacks was performed by analyzing the literature on attack quantification and the characteristics of the DAS environment. A modeling method for quantifying DAS attacks based on the CVSS and an AT was presented, and its feasibility was verified through experiments.

To our best knowledge, this work is the first to quantify attack value by ATs in DASs. The AT model is very suitable for DASs hierarchical features in architecture. The experimental results show that the proposed model can reduce the influence of subjective factors on attack quantification, improve the probability of predicting attacks on the DASs, generate attack paths, better characterize attack characteristics, and determine the attack path and quantification probability. The quantitative results of the model's evaluation can find the most vulnerable component of a DAS and provide an important reference for developing targeted defensive measures in DASs.

Author Contributions: Conceptualization, E.L. and C.K.; methodology, D.H., M.H., and X.L.; validation, F.C., L.H., D.H., and M.H.; formal analysis, E.L. and D.H.; investigation, C.K. and D.H.; resources, E.L. and X.L.; writing—original draft preparation, D.H.; writing—review and editing, E.L., X.L., and C.K.; supervision, X.L.; project administration, E.L. and X.L.; funding acquisition, E.L. and C.K.

Funding: This research was supported in part by the project "Research on Security Architecture for Next Generation Distribution Automation System" of the State Grid Corporation of China and was partly supported by the National Nature Science Foundation of China (61672111).

Acknowledgments: The authors would like to convey their heartfelt gratefulness to the reviewers and the editor for their valuable suggestions and important comments that greatly helped to improve the presentation of this manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Dobson, P.; Koerner, L.; Vaz, R. Venezuela: Guaido stripped of immunity, protests erupt over blackouts. *Green Left Weekly* **2019**, *1216*, 13.
2. Zhou, L.; Ouyang, X.; Ying, H.; Han, L.; Cheng, Y.; Zhang, T. Cyber-Attack Classification in Smart Grid via Deep Neural Network. In Proceedings of the 2nd International Conference on Computer Science and Application Engineering, Hohhot, China, 22–24 October 2018.
3. Sun, C.C.; Hahn, A.; Liu, C.C. Cyber security of a power grid: State-of-the-art. *Int. J. Electr. Power Energy Syst.* **2018**, *99*, 45–56. [CrossRef]
4. Zhao, Y.; Bai, M.; Liang, Y.; Ma, J.; Deng, P. Fault Modeling and Simulation Based on Cyber Physical System in Complex Distribution Network. In Proceedings of the 2018 China International Conference on Electricity Distribution (CICED), Tianjin, China, 17–19 September 2018; pp. 1566–1571.
5. Ciapessoni, E.; Cirio, D.; Massucco, S.; Morini, A.; Pitto, A.; Silvestro, F. Risk-based dynamic security assessment for power system operation and operational planning. *Energies* **2017**, *10*, 475. [CrossRef]
6. Huang, K.; Zhou, C.; Qin, Y.; Tu, W. A Game-Theoretic Approach to Cross-Layer Security Decision-Making in Industrial Cyber-Physical Systems. *IEEE Trans. Ind. Electron.* **2019**. [CrossRef]
7. Huang, W.; Liu, Q.; Yang, S.; Xiong, W.; Liu, Z. Security situation awareness based on power-supply ability model of active distribution system. *Electr. Power Autom. Equip.* **2017**, *37*, 74–80.
8. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [CrossRef]
9. Wang, Q.; Pipattanasomporn, M.; Kuzlu, M.; Tang, Y.; Li, Y.; Rahman, S. Framework for vulnerability assessment of communication systems for electric power grids. *IET Gener. Transm. Distrib.* **2016**, *10*, 477–486. [CrossRef]
10. Kateb, R.; Tushar, M.H.K.; Assi, C.; Debbabi, M. Optimal tree construction model for cyber-attacks to wide area measurement systems. *IEEE Trans. Smart Grid* **2018**, *9*, 25–34. [CrossRef]
11. Wang, X.; Sun, B.; Liao, Y.; Xiang, C. Computer Network Vulnerability Assessment Based on Bayesian Attribute Network. *J. Beijing Univ. Posts Telecommun.* **2015**, *38*, 106–112.
12. Miao, F.; Zhu, Q.; Pajic, M.; Pappas, G.J. A hybrid stochastic game for secure control of cyber-physical systems. *Automatica* **2018**, *93*, 55–63. [CrossRef]
13. Yan, F.; Yin, X.; Huang, H. Research on establishing network intrusion modeling based on MLL-AT. *J. Commun.* **2011**, *32*, 115–124.
14. Zhang, H.; Wu, Z.; Ge, F.; Rong, X.; Yang, W.; Xu, C. Research on Power Distribution Automation Construction Effects Evaluation System Based on SMART Criteria. *Power Syst. Technol.* **2016**, *40*, 2192–2198.
15. Luo, F.; Yang, W.; Zhang, T.; Wang, C.; Wei, G.; Yao, L. Influence of Distribution Automation Data Transmission Errors on Power Supply Reliability of Distribution System. *Autom. Electr. Power Syst.* **2018**, *42*, 10–19.
16. Schneier, B. Attack trees. *Dr. Dobb's J.* **1999**, *24*, 21–29.
17. Lallie, H.S.; Debattista, K.; Bal, J. An empirical evaluation of the effectiveness of attack graphs and fault trees in cyber-attack perception. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1110–1122. [CrossRef]
18. Kong, H.K.; Hong, M.K.; Kim, T.S. Security risk assessment framework for smart car using the attack tree analysis. *J. Ambient Intell. Hum. Comput.* **2018**, *9*, 531–551. [CrossRef]
19. Doynikova, E.; Kotenko, I. CVSS-based probabilistic risk assessment for cyber situational awareness and countermeasure selection. In Proceedings of the 2017 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), St. Petersburg, Russia, 6–8 March 2017; pp. 346–353.
20. Venkataramanan, V.; Srivastava, A.; Hahn, A.; Zonouz, S. Enhancing Microgrid Resiliency Against Cyber Vulnerabilities. In Proceedings of the 2018 IEEE Industry Applications Society Annual Meeting (IAS), Portland, OR, USA, 23–27 September 2018; pp. 1–8.
21. Aksu, M.U.; Dilek, M.H.; Tatlı, E.İ.; Bicakci, K.; Dirik, H.İ.; Demirezen, M.U.; Aykır, T. A quantitative CVSS-based cyber security risk assessment methodology for IT systems. In Proceedings of the 2017 International Carnahan Conference on Security Technology (ICCST), Madrid, Spain, 23–26 October 2017; pp. 1–8.
22. Common Vulnerability Scoring System v3.0: User Guide. Available online: https://www.first.org/cvss/v3.0/user-guide (accessed on 19 June 2019).

23. Moussa, B.; Debbabi, M.; Assi, C. A detection and mitigation model for PTP delay attack in an IEC 61850 substation. *IEEE Trans. Smart Grid* **2018**, *9*, 3954–3965. [CrossRef]
24. Li, X.; Ma, H.; Zhou, F.; Gui, X. Service operator-aware trust scheme for resource matchmaking across multiple clouds. *IEEE Trans. Parallel Distrib. Syst.* **2015**, *26*, 1419–1429. [CrossRef]