Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 6442778, 16 pages
https://doi.org/10.1155/2022/6442778

Research Article

A Prioritizing Interdiction Surface-Based Vulnerability Remediation Composite Metric for Industrial Control Systems

Zibo Wang,[1,2] Yaofang Zhang,[1,2] Zhiyao Liu,[3] Tongtong Li,[1,2] Yilu Chen,[1,2] Chen Yang,[4] Bailing Wang,[1,2,5] and Zhusong Liu[6,7]

[1] *School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China*
[2] *School of Cyber Science and Technology, Harbin Institute of Technology, Harbin 150001, China*
[3] *China Industrial Control Systems Cyber Emergency Response Team, Beijing 100040, China*
[4] *Institute of Software, Chinese Academy of Sciences, Beijing 100190, China*
[5] *Weihai Cyberguard Technologies Co. Ltd, Weihai 264209, China*
[6] *School of Computer Science and Technology, Anhui University of Technology, Anhui 243002, China*
[7] *School of Computer Science, Guangdong University of Technology, Guangzhou 510006, China*

Correspondence should be addressed to Chen Yang; yangchen@iscas.ac.cn and Bailing Wang; wbl@hit.edu.cn

Received 16 March 2022; Revised 25 April 2022; Accepted 30 April 2022; Published 29 May 2022

Academic Editor: Junjuan Xia

Recently, industrial control system (ICS) has gradually been a primary attack target. The main reason is that increasing vulnerabilities exposed provide opportunities for launching multistep and multihost attacks to breach security policies. To that end, vulnerability remediations are crucial for the ICS. However, there exist three problems to be tackled in a sound way. First of all, it is impractical to remove all vulnerabilities for preventing the multistep and multihost attacks in the consideration of the actual ICS demands. Secondly, ranking vulnerability remediations lacks a guidance. The last problem is that there is a lack of a metric for qualifying the security level after each remediation. In this paper, an ICS-oriented assessment methodology is proposed for the vulnerability remediations. It consists of three phases corresponding to the above problems, including (1) prioritizing Interdiction Surfaces, (2) ranking vulnerability remediations, and (3) calculating composite metrics. The Interdiction Surface describes a minimum set of vulnerabilities of which the complete removal may interdict all discovered attack paths in the system. Particularly, it innovates to take the urgent security demands of the ICS into account. Subsequently, ranking the vulnerability in the optimal Interdiction Surface is conducive to guide the remediations with the priority. A composite metric is ultimately given to assess the security level after vulnerability remediations. The effectiveness of the proposed methodology is validated in an ICS scenario which is similar to the real-world practice. Results show that the entire procedure is suitable for the context of the ICS. Simultaneously, the composite metric enhances both the comprehensiveness and the compatibility in contrast with attack path-based metrics. Hence, it overcomes the shortcomings when they are used in isolation.

1. Introduction

For the past few years, security incidents of the industrial control system (ICS) have shown an upward trend with the integrations of emerging technologies in development such as Cloud Computing and Internet of Tings (IoT) [1]. As a side effect of such technologies, more and more vulnerabilities in hardware, software, or policies are brought into the ICS, which allows attackers to gain unauthorized access to the system. However, sophisticated attackers are not satisfied to exploit single vulnerability any longer, and they instead launch multistep and multihost attacks with multiple vulnerabilities, posing a greater threat [2, 3].

Correspondingly, security analysts build the vulnerability-oriented model to be aware of possible exploitability behaviors from two aspects. One is for single vulnerability [4], and the other is for chained ones [5]. To have a deep insight on interactions among various vulnerabilities, attack path- (AP-) based analysis is a typical approach for the ICS. It reveals potential risk dependencies among assets in the system, which is crucial for vulnerability remediations.

An initial idea of our work originates from urgent demands of security practitioners in the ICS about vulnerability remediations. They anticipate getting a security metric that is a quantitative measure of the security level after each remediation, which is of importance to assess the residual risks in the system. A variety of security metrics that play an importantly auxiliary role in the vulnerability remediations were proposed by previous relevant work [6]. Nevertheless, none of these existing isolated metrics are capable to directly be applied into the ICS, because it neglects the relevant demands whose descriptions are summarized briefly.

(D1) In order to prevent the attacks from the context of the ICS, interdicting all discovered APs is more feasible than removing all vulnerabilities in practice. Since a lack of a valid patch for the "0 Day" or a remote access is very common in the ICS, remediations for all vulnerabilities appear to be difficult compared to conventional information technology (IT) systems.

(D2) The disruption to the industrial process will be avoided if the multistep and multihost attacks are detected and eliminated in the early stage. In other words, each AP is interdicted as soon as possible so that the complete chain of vulnerabilities fails to form and reach the goal.

(D3) Remediations focus on as few vulnerabilities as possible, owning to the cost of vulnerability removals and limited budgets for the security maintenance. As we all know, the cost is constrained by the budgets, particularly for industrial manufacturers.

(D4) Most importantly, minimal impacts on the ICS components are ought to be taken into account while implementing the security measures mentioned above. After all, it means a considerable cost if the continuous operations of the ICS components such as the Programmable Logic Controller (PLC) and the Distributed Control System (DCS) are affected and even forced to shut down.

As a result, an ICS-oriented assessment methodology is proposed for the vulnerability remediations in our work. Firstly, a vulnerability-oriented attack graph (AG) is constructed. Then, we define an Interdiction Surface including vulnerabilities that may be remedied to eliminate APs in the consideration of the demands mentioned above, and the optimal one is selected by prioritizing. Subsequently, the vulnerabilities in the optimal Interdiction Surface are ranked, which determines the priority to be remedied. Finally, a specific calculation procedure is given for the composite metric of the system.

The contribution of this paper is summarized as follows.

(C1) The proposed concept, namely, Interdiction Surface, is more suitable for the context of the ICS because it caters to the demands of security practitioners. Simultaneously, it establishes a sound foundation for the vulnerability remediations in the further step.

(C2) The proposed composite metric overcomes the shortcomings of the existing metrics used in isolation, which fuses multiple well-known methods to enhance both the comprehensiveness and the compatibility of the AP-based metrics.

(C3) The proposed calculation procedure and each principle for prioritizing Interdiction Surface and ranking vulnerability remediations are explicit and easy to implement, which is conducive for the ICS practitioners to assess the security level after each remediation.

The rest of paper is organized as follows. In Section 2, the related work in the recent literature is reviewed. Section 3 provides some preliminaries to support relevant statements in our work. In Section 4, we describe the proposed methodology and elaborate it by a simple example. Section 5 demonstrates the experiment results in a case study close to the ICS in reality. Ultimately, we conclude the whole paper and provide the future research direction in Section 6.

2. Related Work

In the past two decades, the AP analysis has been attracting the growing interests from quantities of scholars and practitioners in the security vulnerability field. Among the researches on AP analysis, cut set-based methodologies are widespread to analyze critical APs for systems exposed to security threats. To assess threats, security metrics are imperative to measure the security. In this section, the related work is reviewed from the recently published research literature.

2.1. AP Analysis in the ICS. At present, the most mainstream model of the AP analysis is the AG. AG is a kind of formalized mathematical representation of how an attacker reaches final malicious goals by exploiting a set of vulnerabilities that constitute a multistep and multihost attack. Prioritizing APs is transformed to the discovery of critical nodes or edges in the AG for making sense of intrusion intentions, hardening systems, or mitigating risks [7–11]. From the perspective of AP-based applications in the ICS, typical analyzing approaches are estimating the node importance, i.e., the PageRank algorithm, and employing probabilistic graphical models, i.e., Markov Chain.

Nevertheless, performing the AP analysis for the ICS needs to make more effort on additional considerations of its scene characteristics. Stellios et al. modeled both the cyber connectivity and physical interactions to prioritize APs, no matter which AP is hidden or underestimated at risks [5]. Barrère et al. built AND/OR dependency graphs to identify a minimal number of the ICS components with overlapping security measures or critical missions [12, 13]. Considering the cost of remediations and security budgets for securing the IoT, Yiğit et al. leveraged a compact AG to construct a cost-effective protecting strategy applied to the large-scale environment [14]. Stergiopoulos et al. extracted graph series and utilized group clustering to analyze the risk of the entire network, concerning complexity and interactions of the complex networks in Industry 4.0 [15]. In our work, we likewise integrate the component impact into the proposed methodology as an ICS characteristic.

2.2. Cut Set-Based Methodologies. Cut set is a vital concept in the graph theory, which usually applies to security research fields such as network reliability and defense hardening. Identifying a cut set is a desirable means to prevent an attacker from reaching the final goal under the circumstance of appropriate security countermeasures, which is employed into the AP analysis.

There is no doubt that the cut set-based methodology appears in the context of the ICS to guarantee the system security as well. Incorporating the promising defense-in-depth principle, Mell et al. generated a colored AG that represents known vulnerability types in the ICS network [16]. And then, the problems of the shortest color path and the minimum color cut set were settled, exactly measuring both of the depth and the width and promoting the security posture. Ghazo and Kumar presented a discovering approach of critical-attack set for a supervisory control and data acquisition (SCADA) system based on the minimum-label cut set [17]. The minimum number of labels was obtained by a set of backward reachable strongly connected components. George and Thampi focused on the vulnerability-based assessment for edge devices of the IoT-assisted networks [18, 19]. A graphical model was formulated to isolate target devices from the attackers by a minimum cut set of vulnerabilities. In this regard, our research objective is similar.

In the point view of the game theory, an attacker looks forward to choosing the AP with the least amount of cost, whereas the optimal defensive investments allocated on the basis of the minimum cut sets may expand that cost. Such described scenario is an instance of problem called Interdiction Network [20–22]. Originally, the problem concerns on the interdiction between attackers and defenders. Attackers act as leaders to deteriorate the network performance by determining the best edge cut set [21] or k-critical ones [22]. In contrary, defenders act as followers to strengthen the targeted network. In our work, we introduce the analogous idea to define a concept named Interdiction Surface, which is customized for the ICS. The difference is that the defenders refer to interdicting all APs along with the vulnerability remediations.

2.3. Security Metrics. Security metrics for system-level security cover four aspects including system vulnerabilities, defense power, severity of attack or threat, and situations [23]. Our work focuses on the metrics of system vulnerabilities that can be further classified into individual-vulnerability-oriented ones such as metrics in the common vulnerability scoring system (CVSS, https://www.first.org/cvss/) and multiple-vulnerability-oriented ones such as the AP-based metrics.

Most of the existing metrics are aimed at the business process and internal network of enterprise IT system [24–26] rather than the ICS. But the security metrics in the ICS are essential for the AP analysis with a quantitative measure. The aforementioned literature regarding the ICS [12, 14] can be used to prove that point. In [12], the metric captures the security measure instances and is defined on a logical formulation transformed from the AND/OR graph. Afterwards, the variables in the formulation are assigned a compromise cost. In [14], the metric is the sum of the likelihoods of the APs, which guides the allocation of security budgets for the ICS. More generally, certain existing AP-based metrics are pointed out obvious drawbacks used in isolation, thus confusing security analysts to make wrong decisions, which is absolutely intolerable for the ICS [6]. Hence, a composite metric is proposed in our work to improve the deficiencies, especially for the security-level assessment.

3. Preliminary

In this section, we will briefly introduce a series of fundamental concepts to assist readers interested in the proposed approach. As building blocks, the basic terminologies and definitions are provided for further elaboration.

3.1. Vulnerability-Oriented Attack Graph. Since we seek to interdict as many APs as possible by removing vulnerabilities, vulnerability-oriented AG is adopted into the proposed approach. Its advantage is explicitly representing some vulnerabilities on a device, which makes it intuitive to figure out a chain of vulnerabilities to compromise a target system. The vulnerability-oriented AG is described as follows:

(i) Vulnerability-oriented AG: given a directed acyclic $\mathbf{AG} = (\mathbf{S}, \mathbf{E}, S_0, T)$, where $\mathbf{S} = \{S_i | i = 1, 2, \cdots, n\}$ is a set of nodes, $\mathbf{E} \subseteq \mathbf{S} \times \mathbf{S}$ is a set of edges that connect between pairs of nodes, S_0 is a source node, and T is a terminal node. The node in the AG represents an affected component running on a specific device, and the directed edge represents an exploitation of the vulnerability. Assume that S_0 is a compromising entry point of an attack, and T is a malicious goal that violates system

In fact, an attacker exploits each vulnerability with a varying difficulty level. Hence, vulnerabilities have different probabilities of being successfully exploited. In our work, we extract the empirical Exploitability Score (ES) from the CVSS to calculate Vulnerability Exploitability Probability. The definition is given as follows.

(ii) Vulnerability Exploitability Probability (VEP): the metrics of the ES consist of Attack Vector (AV), Attack Complexity (AC), Authentication (Au), and User Interaction (UI), where $\mathrm{ES} = 8.22 \times \mathrm{AV} \times \mathrm{AC} \times \mathrm{Au} \times \mathrm{UI}$. Exploitability probability EP is derived from the normalization of ES

3.2. Absorbing Markov Chain. Exploitation is a stochastic process in a multistep and multihost attack. Its probability of transition from one state to another is determined by the state of the current vulnerability. With the help of various privileges from vulnerabilities, an attacker may reach new state until realizing the final malicious goal. Therefore, such attack process is effectively described as an Absorbing Markov Chain. Some relevant terminologies and definitions are provided as follows:

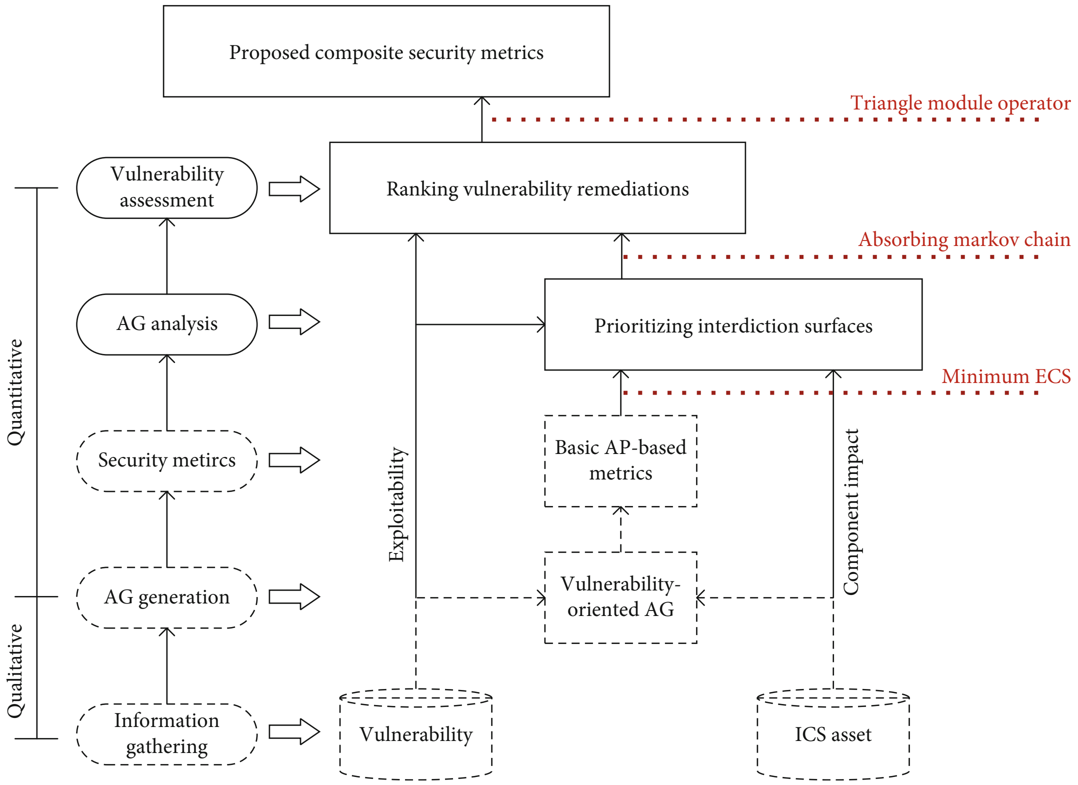


Figure 1: Overview of the proposed methodology.

(i) Markov Property: considering a discrete stochastic sequence including a finite number of states, $\mathbf{X}=\{x_1, x_2,\cdots,x_n\}$, if an equation $P(x_{i+1}|x_i, x_{i-1},\cdots x_1)=P(x_{i+1}|x_i)$ is always satisfied where $P(x_{i+1}|x_i)$ denotes the probability of transition from x_{i+1} to x_i, it is defined as Markov Property. The sequence is called a Markov Chain

If there exist two states x_i and x_j in the Markov Chain $\mathbf{X}$, the transition probability $P(x_i|x_j)$ could be denoted as P_{ij} for short. Similarly, P_{ii} represents the probability of a transition to the state x_i itself.

(ii) Absorbing Markov Chain (AMC): if the state x_i can only transfer to itself and $P_{ii}=1$, the state x_i is defined as an absorbing state. And other states of $\mathbf{X}$ could transfer to the absorbing state in finite times. Thus, the chain $\mathbf{X}$ is subsequently called AMC. Simultaneously, all transition probability for each state in the AMC should be added up to 1 [24]

3.3. Edge Cut Set. The cut set in the graph theory is classified into the node cut set and the edge cut set. The removal of nodes or edges in the set has an effect on the connectivity between certain nodes in a graph. According to the requirements of our work, the formal definitions on the edge cut set are overviewed.

(i) Edge cut set (ECS): given all nodes of a directed graph $\mathbf{G}$ are in a set $\mathbf{N}$, a cut divides $\mathbf{N}$ into two parts, $\mathbf{D}$ and $\bar{\mathbf{D}}=\mathbf{N}-\mathbf{D}$. The cut represents a set of edges, namely, ECS. Among them, each edge has a feature that one endpoint is in the set $\mathbf{D}$ and the other endpoint is in the set $\bar{\mathbf{D}}$

In other words, the definition indicates that collective removal of those edges from the graph G will disrupt node connectivity. Obviously, the ECS is not unique, since any set containing an ECS is also an ECS. To some extent, it is convenient for further analysis to reduce the number of the ECSs. Then, minimum ECS refers to as follows.

(ii) Minimum ECS: it is defined as an edge cut set satisfying that all strict subsets are not cut sets

3.4. Attack Path-Based Metrics. The AP-based metric may quantify the overall security of a system such as the network topology, vulnerabilities of services, weaknesses of protocols, as well as defense policies. It is roughly classified into two categories. One is intuitively obtained from the vulnerability-oriented AG, just as the following three typical metrics described [6, 23]:

(i) Number of APs: specifically, it is the number of complete paths in the vulnerability-oriented AG, defined as $\text{Num}_{\text{APs}}=|p_1, p_2,\cdots,p_n|$, where p_n denotes each AP. This metric is the total number of ways that an attacker leverages chained exploits

(ii) Shortest AP: this metric is the shortest length from an initial node to the same goal, defined as Len_{SAP}

$= \min\left[\mathrm{len}(p_1), \mathrm{len}(p_2), \cdots, \mathrm{len}(p_n)\right]$, where $\mathrm{len}(\cdot)$ denotes the length of each AP. It indicates that the minimum number of vulnerabilities is exploited to launch a multistep attack

(iii) Expectation of AP lengths: this metric is the arithmetic average of all AP lengths computed over the AG, which is defined as follows. It gives the expected effort of compromising a targeted system

$$\mathrm{Exp}_{\mathrm{APlen}} = \frac{\sum_{i=1}^{n} \mathrm{len}(p_i)}{\mathrm{Num}_{\mathrm{APs}}} \tag{1}$$

By assigning values of expert experience on vulnerability, the other category metric takes account of the probability of AP. The cumulative probability of each exploit on the AP captures the likelihood to reach the final goal. Considering the AMC and the VEP, the following definition is given.

(iv) Probability of AP: given a vulnerability-oriented AG mapped into an AMC, P_{APMarkov} denotes the probability of an AP, which is defined as

$$P_{\mathrm{APMarkov}} = \prod_{i=1}^{m} P_M(\mathrm{EP}_i), \tag{2}$$

where m is the number of vulnerabilities included in the AP. $P_M(\mathrm{EP}_i)$ denotes the transition probability of the AMC regarding the VEP whose specific calculation method is introduced in [24].

Despite the metrics mentioned in this subsection which provides referable results in security evaluation, they also could not meet a comprehensive demand, even misleading analysts, when utilized in isolation [6]. In the next section, we will discuss the shortcoming of these metrics in detail and present our novel metric for vulnerability remediations.

4. Proposed Methodology

As detailed ahead, the unique characteristics of the ICS such as the operational continuity and the limited budget for the security maintenance pose numerous obstacles for security analysts. In addition, it is impractical to eliminate all vulnerabilities in the ICS for the sake of techniques and costs. In terms of these two aspects, the proposed methodology intends to develop a novel security metric to provide a sound guidance for the vulnerability assessment, which is suitable for prioritized remediation requirements in the context of the ICS.

The overview of the proposed methodology is illustrated in Figure 1. We perform from a qualitative analysis to the quantitative one based on the AG modeling with information on the ICS assets and potential vulnerabilities. Interdicting APs with a fraction of vulnerabilities discovered for a given system is a conducive way instead of removing all vulnerabilities in the current security practice. For that reason, we optimize both the selection of vulnerability collection and the sequence of handling them, taking into consideration business impacts on ICS components and the efficiency of eliminating APs. Combined with a series of basic AP-based metrics, a composite metric is generated to improve the ability of capturing the security level in the wake of vulnerability remediations. The proposed methodology is divided into three phases as follows.

(P1) Prioritizing Interdiction Surfaces: in this phase, a concept "Interdiction Surface" is proposed to describe a collection including a relatively small number of vulnerabilities to be removed for the purpose of eliminating APs in the ICS. This concept is supported by the definition of the minimum ECS in the graph theory; however, the difference is that it considers the factor of business impacts on relevant ICS components. What is more, a specific calculation method is introduced to select an interdiction surface among plenty of similar results in a prioritizing manner.

(P2) Ranking vulnerability remediations: the primary goal of the phase is to rank each vulnerability which is a member of the optimal Interdiction Surface at present. The vulnerability-oriented AG of the given ICS is mapped into an AMC. Depending on two types of the typical AP-based metrics mentioned in the last section, each removal of the vulnerability is scored according to the contribution to eliminating as many APs as possible and decreasing the probability to accomplish a multistep attack. On the other side, it indicates less exploitable opportunities once the vulnerability is priority to be remedied.

(P3) Calculating composite security metrics: the ultimate goal of the phase is to quantify security level after removing a vulnerability selected in the P2. In order to avoid the drawbacks in single using of existing AP-based metrics mentioned in the previous literature, a composite metric is designed to assess security level in a holistic view. On the basis of Triangle Module Operator, we integrate the intermediate results which are in the first two phases together from three aspects, including the ranking level of each vulnerability in the prioritized interdiction surface, the transition probability, and the changes of the basic AP-based metrics before and after the removal of a specific vulnerability.

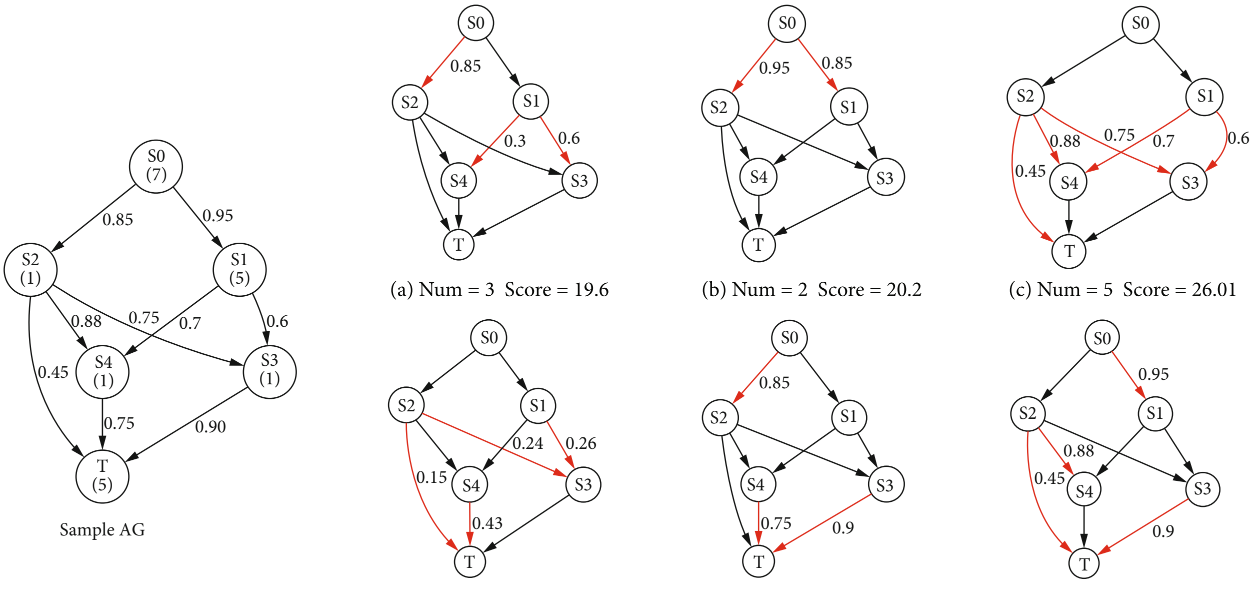
4.1. Prioritizing Interdiction Surfaces. Based on these four security demands of the ICS described in Introduction, we propose a concept called "Interdiction Surface" and then give an algorithm to prioritize such surfaces. Before the statements regarding the proposed methodology in this part, there are four targeted responses to the demands (D1~D4) with the help of the preliminaries in Section 3.

(R1) Recall that the minimum ECS is a set of edges whose collective removal ensures a graph divided into two parts. Incorporating the concept of the graph theory into the vulnerability-oriented AG, all APs are interdicted by removing a specific set whose members represent vulnerabilities to be remedied.

(R2) Each AP in our work is treated as a sequential chain of vulnerabilities. If the vulnerability located closely to the initial point of the entire chain is remedied, the AP could be interdicted as soon as possible. The shortest AP metric captures the phenomenon in a quantitative way.

```
Input: a vulnerability-oriented AG, a list of the VEPs, a list of impact value on the ICS components
Output: an optimal Interdiction Surface
get the edge set E, the node set S, the initial nodes $S_0$ and terminal node $T$ from the AG
for an edge in the Edo
        assign the Grade to each edge in the S
End for
initialize a set IS and then store each edge set with the same Grade into the set
initialize a set RL
for an edge in the Edo
        store the relation of edges satisfying the Root-Leaf in the RL
End for
for a member in the ISdo:
        replace the root edge in RLwith the leaf edge in the different grade to generate cut sets P
        conduct the Minimized Testing for each new possible cut set in the P
        if the possible cut set is the Minimum ECS then
        add the possible cut set into the IS
        End if
End for
assign the VEPs and the impact value to each edge and each node
calculate in Eq. (3) for each member in the IS
get the member with the minimum vale of the set of the calculation results
Return
```

Algorithm 1: Prioritizing Interdiction Surfaces.



Sample AG

(a) Num = 3 Score = 19.6

(b) Num = 2 Score = 20.2

(c) Num = 5 Score = 26.01

(d) Num = 4 Score = 27.3

(e) Num = 3 Score = 31.95

(f) Num = 4 Score = 36.01

Figure 2: Illustration for prioritizing Interdiction Surface.

(R3) The set described in R1 is not unique. Meanwhile, each set has varying numbers of members. It is not a trivia to select a set with fewer but probably not the least members in the consideration of many factors offered in D3. It is essential to decide the size of the set referring to other metrics.

(R4) The impacts on the ICS components may also be quantified by multiple of means such as the expert knowledge in the ICS field, historical data on the industrial operation, and inspections from security analysts. The combination of the quantitative values and the VEP guarantees that impacts on the ICS merge into the process of the vulnerability assessment.

Accordingly, the Interdiction Surface is defined in accordance with these responses to the practical demands of the ICS, given as follows:

(i) Interdiction Surface: the virtual surface depicts a way to cut off all discovered APs, which consists of minimal set of vulnerabilities to be remedied. Its selection

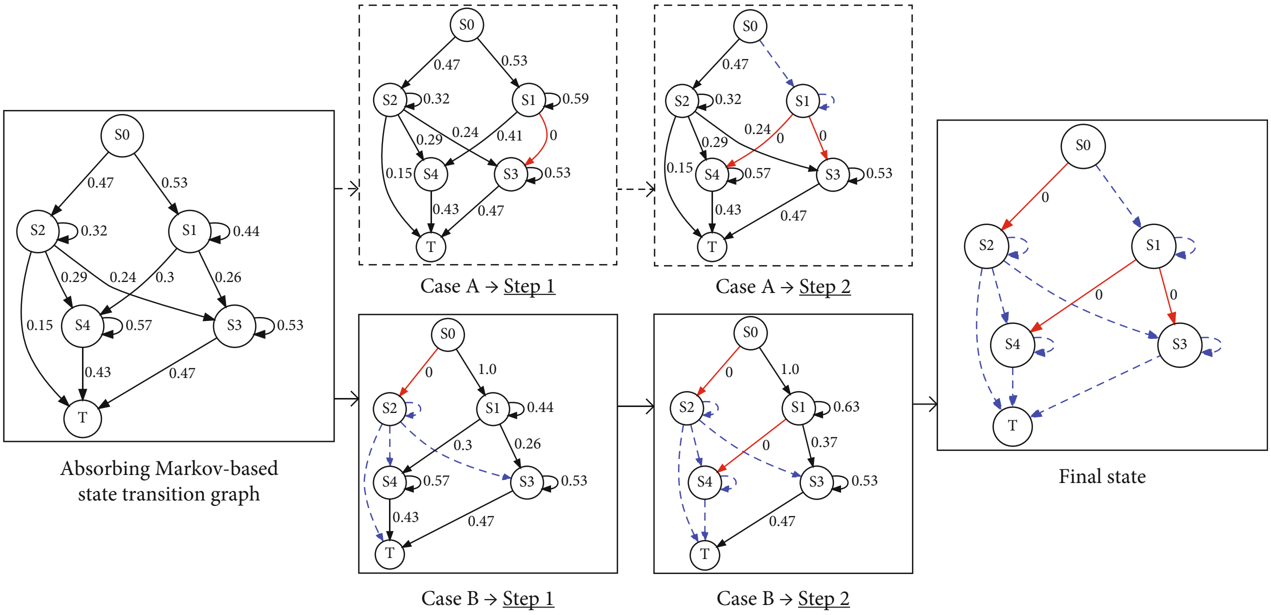


Figure 3: Illustration for removing the edges.

Table 1: AP metrics for case A.

AP-based metrics	Initial conditions	$S_1 \longrightarrow S_3$	$S_1 \longrightarrow S_4$	$S_0 \longrightarrow S_2$
Number of APs	5	4	3	0
Shortest AP	2	3	3	0
Expectation of AP lengths	2.8	3.75	3.667	0
Sum of probability of the eliminated APs	—	0.207	0.218	0.575

Table 2: AP metrics for case B.

AP-based metrics	Initial conditions	$S_0 \longrightarrow S_2$	$S_1 \longrightarrow S_4$	$S_1 \longrightarrow S_3$
Number of APs	5	2	1	0
Shortest AP	2	4	4	0
Expectation of AP lengths	2.8	4	4	0
Sum of probability of the eliminated APs	—	0.575	0.218	0.207

among the similar surfaces must comprehensively follow the principles including the shortest AP metric of a given vulnerability-oriented AG, fewer vulnerabilities, and the impacts on the ICS components, which is formulize as

$$\mathrm{Score}_{\mathrm{IS}} = \mathrm{Cut}_{\mathrm{num}} + \sum_{i \in \mathrm{IS}} \mathrm{Cut}_{\mathrm{loc}}(i) + \sum_{i \in \mathrm{IS}} \mathrm{Com\_impact}(i), \quad (3)$$

where $\mathrm{Cut}_{\mathrm{num}}$ denotes the number of vulnerabilities in the Interdiction Surface and $\mathrm{Cut}_{\mathrm{loc}}(i)$ denotes the length of the shortest AP between S_0 and each member of the Interdiction Surface. The impacts on the ICS components are denoted as

$$\mathrm{Com\_impact}(i) = \left(\mathrm{com\_impact}_S + \mathrm{com\_impact}_T\right) \times \mathrm{EP}_i, \quad (4)$$

where $\mathrm{com\_impact}_S$ and $\mathrm{com\_impact}_T$ denote the impacts on a pair of the ICS components regarding a vulnerability. Note that each edge in the AG represents a vulnerability, and the both endpoints of each edge represent the ICS components to support the business process or industrial operations. Hence, the removal of the vulnerability may have an impact on the ICS components in both core data exchanging and run monitoring.

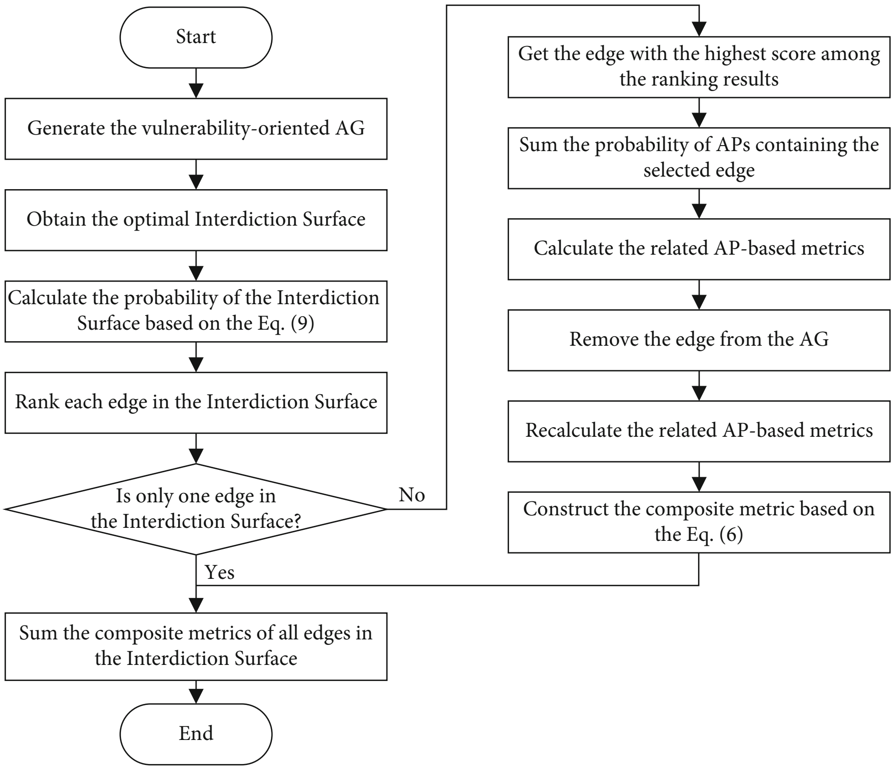

Start
Generate the vulnerability-oriented AG
Obtain the optimal Interdiction Surface
Calculate the probability of the Interdiction Surface based on the Eq. (9)
Rank each edge in the Interdiction Surface
Is only one edge in the Interdiction Surface?
No
Yes
Get the edge with the highest score among the ranking results
Sum the probability of APs containing the selected edge
Calculate the related AP-based metrics
Remove the edge from the AG
Recalculate the related AP-based metrics
Construct the composite metric based on the Eq. (6)
Sum the composite metrics of all edges in the Interdiction Surface
End

Figure 4: A flow chart for calculating the system security metric.

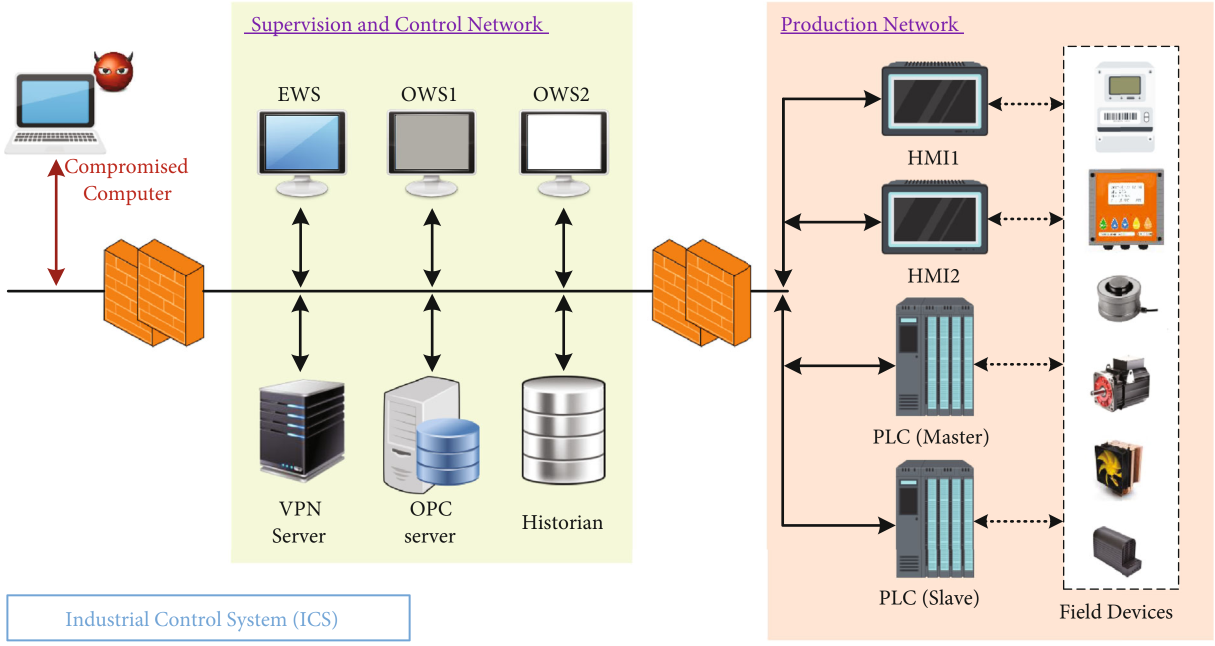


Figure 5: An ICS scenario.

The definition of the Interdiction Surface has a dependence on all minimum ECSs for a given vulnerability-oriented AG. In our work, we utilize the idea of the hierarchical approach in the literature [27] to obtain all minimum ECSs and then determine the prioritizing IS. There are some key concepts of the approach listed in advance.

By means of breadth-first search, each node in a directed acyclic graph is assigned a value called Grade with respect to the minimum number of edges traversed from a given initial node to the node. It is obvious that the sets of nodes with the same grades must be minimum cut sets. Besides, the minimum cut sets including nodes with the different grades is

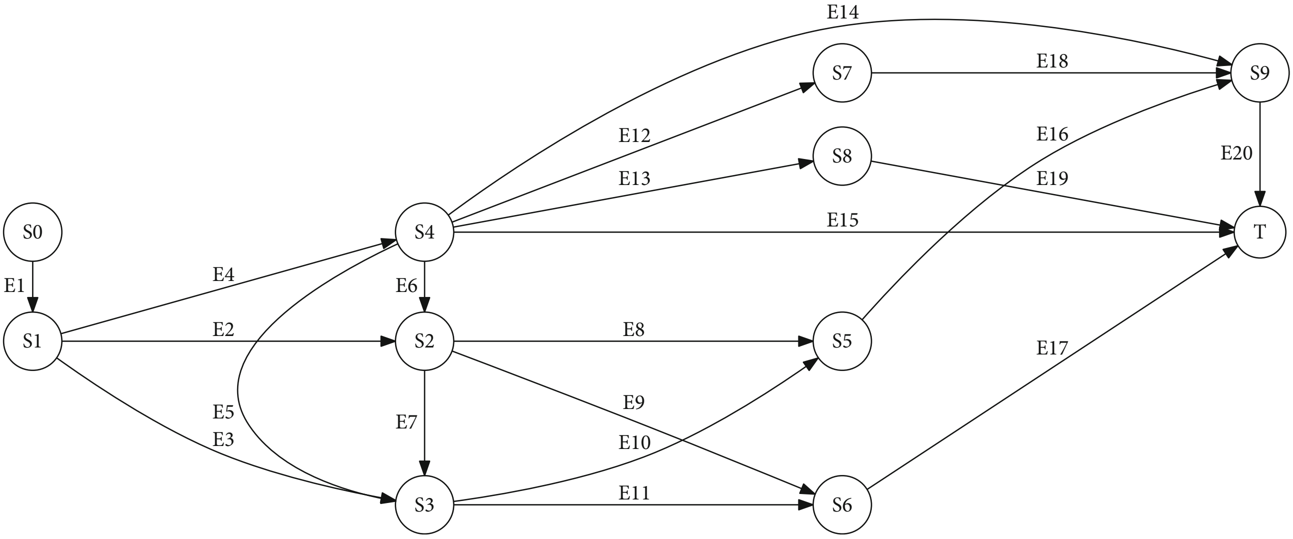


Figure 6: An AG for the ICS.

Table 3: Devices and affected components in the ICS.

Device name	Affected component	Node in AG	Access control	Component impact
Compromised computer	VPN Client	S0	S1	1000
VPN Server	Moxa EDR-G902	S1	S2, S3, S4	10
OPC Server	OPC UA .NET	S2	S3, S5, S6	1
Historian	SIMATIC Process Historian	S3	S5, S6	1
EWS	Windows SMBv3	S4	S2, S3, S7, S8, S9, T	1
OWS1	Siemens Control Center Server Application	S5	S9	1
OWS2	SIMATIC PCS 7	S6	T	1
HMI1	SIMATIC WinCC	S7	S9	9
HMI2	SIMATIC HMI Comfort Panels	S8	T	9
PLC master	SIMATIC S7-1500 CPU	S9	T	10
PLC slave	SIMATIC S7-1200 CPU	T	/	10

Table 4: Vulnerabilities in the ICS.

CVE No.	Edge in AG	ES
CVE-2020-14511	E1	3.9
CVE-2020-29457	E2, E6	0.8
CVE-2021-27395	E3, E5, E7	2.8
CVE-2020-0796	E4	3.9
CVE-2019-19292	E8, E10	2.8
CVE-2021-40359	E9, E11	3.9
CVE-2019-10916	E12	2.8
CVE-2019-6577	E13	2.3
CVE-2020-15782	E14, E16, E18	3.9
CVE-2021-37172	E15, E17, E19, E20	3.9

further explored by using a graphical relation of these nodes called Root-Leaf. On the basis of the grade of nodes, root nodes are taken place of leaf nodes to generate new possible cut sets until all the combinations are traversed. Finally, a minimized testing is conducted for the possible cut sets to ensure that the sets are minimum.

Note that the results in [27] are minimum node cut sets but directly not the minimum ECS in our work. Therefore, we improve the approach and integrate it with the calculation method in Equation (3) to form the proposed Algorithm 1 as follows.

A sample vulnerability-oriented AG is shown in Figure 2, which consists of six nodes and nine edges. S_0 and S_5 denote the source node and the terminal node, respectively, in the AG. The value in parenthesis of each node represents the impact component on the corresponding ICS component, and the value of each edge represents the VEP.

The optimal Interdiction Surface for the sample situation is the edge set $\{S_0 \longrightarrow S_2, S_1 \longrightarrow S_3, S_1 \longrightarrow S_4\}$ with $\text{score}_{\text{IS}} = 19.6$. There are twelve Interdiction Surfaces based on Algorithm 1, six of which are illustrated in Figure 2. The collection of the edges with the red color in each subgraph (a)–(f) denotes the Interdiction Surface. It is observed that the selection of Interdiction Surfaces is a comprehensive process

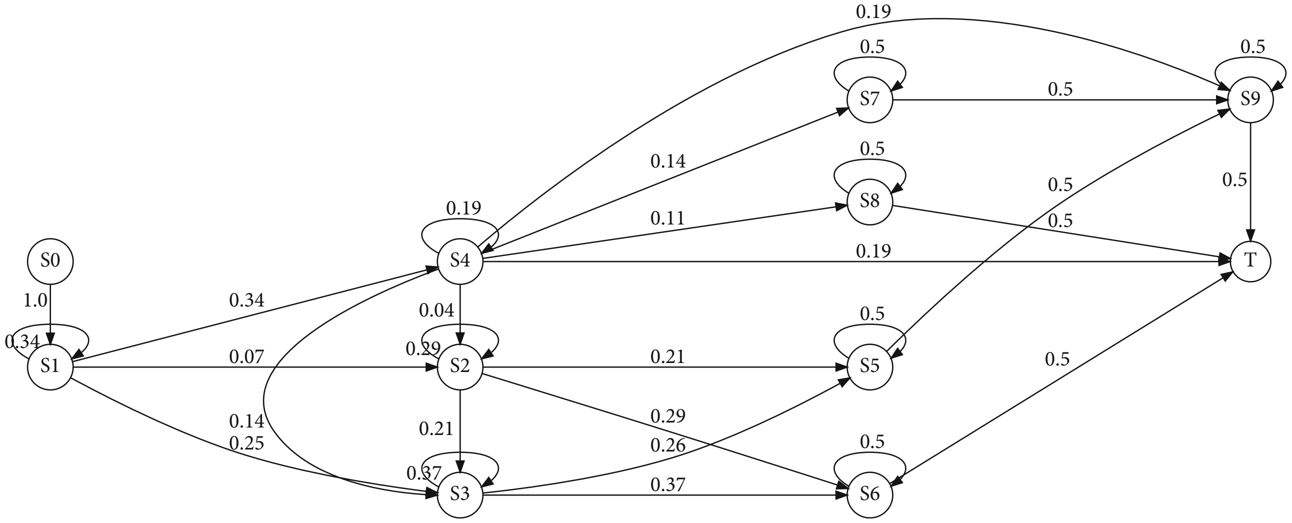


Figure 7: Absorbing Markov-based state transition AG.

Table 5: Top 10 probabilities of AP.

No.	AP	Probability of AP
1	E1, E4, E15	0.06513
2	E1, E3, E11, E17	0.04517
3	E1, E4, E14, E20	0.03256
4	E1, E4, E13, E19	0.01921
5	E1, E3, E10, E16, E20	0.01626
6	E1, E4, E12, E18, E20	0.01172
7	E1, E2, E9, E17	0.01041
8	E1, E4, E5, E11, E17	0.00862
9	E1, E2, E8, E16, E20	0.00375
10	E1, E4, E5, E10, E16, E20	0.00310

Table 6: Top 10 Interdiction Surfaces.

No.	Interdiction surface	Score in P1
1	E2, E4, E10, E11	26.75
2	E2, E3, E4	27.23
3	E4, E8, E9, E10, E11	31.88
4	E2, E4, E10, E17	36.75
5	E3, E4, E7, E8, E9	36.80
6	E4, E8, E10, E17	36.88
7	E2, E4, E11, E16	37.31
8	E4, E9, E11, E16	38.00
9	E4, E16, E17	43.00
10	E2, E4, E11, E20	46.31

without relying on single aspect in Equation (3). For instance, the results are differentiated, even if the number of members in each Interdiction Surface is the same.

4.2. Ranking Vulnerability Remediations. When security analysts have got the optimal Interdiction Surface which enables to eliminate all the APs in the current context of the ICS, a subsequent task is to decide which vulnerability is remedied first. Specifically, concerning on the vulnerabilities in the selected Interdiction Surface, it needs to provide a ranking list of the remediation. And a detailed schedule for the security maintenance is made to coordinate with plans of the industrial production.

In this phase, we employ a mix of more AP-based metrics to rank vulnerability remediations. The reason for the combination of the metrics is that it makes up for the shortcomings when each metric is used alone. For examples, the shortest AP reflects the least effort exerted by an attacker whereas it ignores multiple ways to reach the final goal that is captured by the number of APs. Moreover, the expectation of AP lengths indicates the average efforts made by attackers whereas it ignores the exploit likelihood which is captured by the probability of AP.

Let us proceed to analyze the motivating example. Assuming that only one vulnerability is remedied at a time, we attempt to answer how the sequence of removing each vulnerability in the selected Interdiction Surface has an influence on the AP-based metrics while interdicting all APs. First of all, all APs in the sample AG is mapped into multiple AMCs, forming an absorbing Markov-based state transition graph shown in Figure 3. Note that the value on each edge is relabeled as the transition probability. And then, two cases are illustrated that different sequences of removing edges may achieve the same aim of eliminating all APs in the AG. In this figure, a red solid line denotes a removal of one edge, and a blue dotted line denotes passively a disappearing edge, and the nodes it points to lose all connectivity with other nodes. Compared with these two cases, it is observed that the sequence of removing each edge results in the changes of the transition probability as well as the efficiency to eliminate the APs.

Furthermore, the changes of the AP-based metrics in these two cases are demonstrated in Tables 1 and 2 so as to quantify our discoveries. The first three basic AP-based metrics have the same trend in each case, whereas the rate of the changes is distinctly different. Taking the

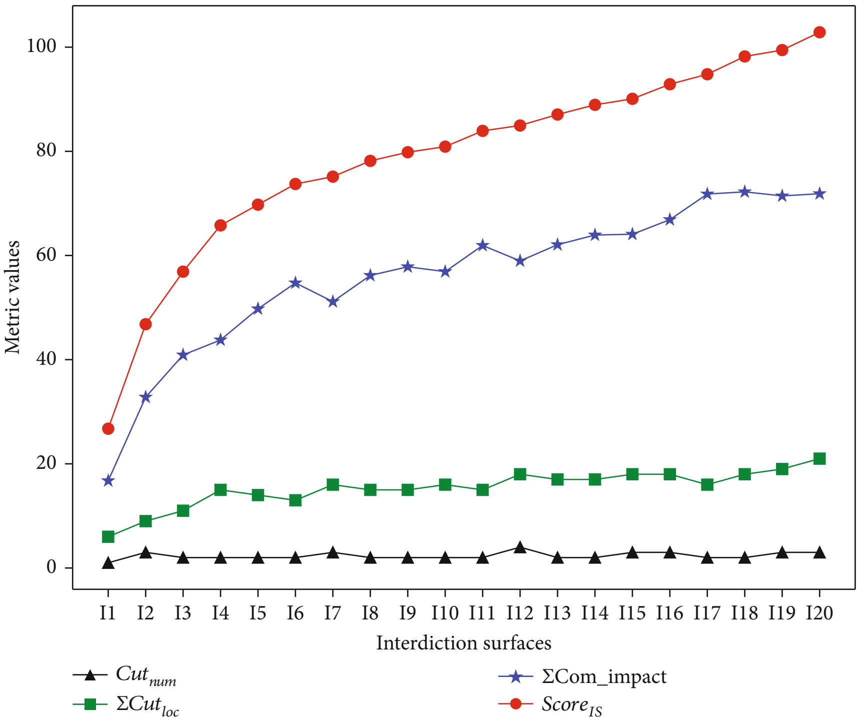


Figure 8: Prioritizing Interdiction Surface.

Table 7: 20 minimum cut sets chosen at random.

No.	Interdiction Surface
I1	E10, E11, E2, E4
I2	E17, E3, E4, E7, E8
I3	E20, E9, E11, E13, E15
I4	E20, E8, E9, E10, E11, E13, E15
I5	E17, E20, E10, E6, E13, E15
I6	E2, E19, E20, E11, E6, E15
I7	E3, E7, E8, E9, E5, E13, E15, E20
I8	E2, E19, E20, E10, E11, E6, E15
I9	E17, E2, E20, E6, E12, E13, E15
I10	E3, E20, E7, E9, E5, E12, E13, E15
I11	E2, E19, E20, E11, E6, E12, E15
I12	E6, E5, E12, E13, E14, E15, E16, E17
I13	E17, E2, E18, E10, E6, E13, E14, E15
I14	E16, E2, E19, E11, E6, E12, E14, E15
I15	E7, E8, E9, E11, E12, E15, E19, E20
I16	E8, E9, E10, E11, E14, E15, E18, E19
I17	E17, E3, E19, E7, E20, E5, E15
I18	E17, E3, E19, E7, E20, E6, E5, E15
I19	E3, E7, E8, E9, E5, E12, E15, E19, E20
I20	E3, E7, E8, E6, E5, E12, E14, E15, E17, E19

number of APs as an example, its value of each step decreases more in case B than that in case A, which means attackers may have less opportunities to reach their expected goal. In particular, we quantify the cumulative effect resulted from the removal of each edge by summing the probability of eliminated APs. Similarly, from the decrease of sum, it is more significant by removing the edge $S_0 \longrightarrow S_2$ in case B than removing the edge $S_1 \longrightarrow S_3$ in case A.

Therefore, two conclusions can be drawn, according to the analysis for the example. One is that it is effective to cope with the problem of this subsection for ranking the vulnerability remediations based on the combination of a series of the AP-based metrics. The other is that the quantifiable changes are able to assess the security level of the whole system. The latter will be described in the next subsection. The former conclusion concerning on a principle for ranking vulnerability remediations is formulized as

$$\mathrm{Socre}_R(\mathrm{Vul}) = 0.33 \times \left[\mathrm{EP} + \mathrm{Num}_{\mathrm{SAP}}(\mathrm{Vul}) + \sum_{i=1}^{k} P_{\mathrm{E-APMarkov}}(i)\right] - \mathrm{Exp}_{\mathrm{APlen}}(\mathrm{Vul}), \tag{5}$$

where $\mathrm{Num}_{\mathrm{SAP}}(\mathrm{Vul})$ denotes the number of the shortest APs with respect to the vulnerability which represents an edge in the AG, k denotes the number of the eliminated APs once removing an edge, $P_{\mathrm{E-APMarkov}}(i)$ denotes the probability of the ith eliminated AP, and $\mathrm{Exp}_{\mathrm{APlen}}(\mathrm{Vul})$ denotes the expectation of AP lengths, and the AP contains the vulnerability. Except for the EP, the other terms in Equation (5) are normalized.

According to the Equation (5), the results are $\mathrm{score}_R(S_0 \longrightarrow S_2) = 0.353$ and $\mathrm{score}_R(S_1 \longrightarrow S_4) = 0.033$. Hence, the ranking result is $(S_0 \longrightarrow S_2) \gg (S_1 \longrightarrow S_4) \gg (S_1 \longrightarrow S_3)$ which is consistent with the previous analysis.

Table 8: Vulnerability remediation metric in each step.

No.	Edge in AG	Score in P2	Composite metric
1	E4	0.54	0.83
2	E11	0.308	072
3	E10	0.051	0.60
4	E2	—	—

4.3. Calculating Composite Security Metrics. At a high level, the security analysts are not satisfied with just ranking the vulnerability remediations. Meanwhile, they pay more attention to some security-relevant attributes the ICS possesses in reality. The attributes in our work concentrate on the AP-based metrics. However, more or less drawbacks exist in such metrics because of their one-sidedness, thus misleading the analysts to make the unreasonable decision. To address that, we propose a composite security metric in the situation of quantifying security level after each vulnerability remediation.

The other conclusion derived from the example is described as follows. Changes in the AP-based metrics are treated as benefits from the vulnerability remediations, which also turns to aggravate much burden on the multistep and multihost attacks. For instance, the decrease in the number of APs as well as the increase in both the expectation of AP lengths and the probability of APs may make the attacker take more and more effort associated with the time and costs until they could not afford and choose to give up the target. It means the system security level is enhanced as well. Apart from the benefits, the ranking results in the **P2** simultaneously affect the security level. The more appropriately vulnerabilities are ranked, the better the effect of preventing the ICS from the attacks can be attained.

To fuse these two aspects including the benefits and the ranking results, we introduce an approach called Triangle Module Operator into the proposed methodology to assess their combined effects on the security of the ICS. The approach has an advantage in fusing heterogeneous functions of different factors related to a system [28]. It strengthens and reconciles these factors to achieve a comprehensive evaluation, in which a single factor could not absolutely dominate in the result. As a result, the approach is suitable to balance the benefits and the ranking results within the composite metric.

The composite metric for a given vulnerability Vul is given as

$$\mathrm{Com\_metric}(\mathrm{Vul}) = \frac{\mathrm{Ra} \times \mathrm{Be}}{1 - \mathrm{Ra} - \mathrm{Be} + 2 \times \mathrm{Ra} \times \mathrm{Be}}, \qquad (6)$$

where $\mathrm{Vul} \in \mathrm{IS}$, Ra denotes the ranking function, and Be denotes the benefit function. The ranking function is defined as

$$\mathrm{Ra} = 1 - \frac{r(\mathrm{Vul})}{\sum_{m \in \mathrm{IS}} r(m)}, \qquad (7)$$

where $r(\cdot)$ represents the ranking result for each member in the Interdiction Surface. The benefit function is defined as

$$\mathrm{Be} = 0.25 \times \left(\sum P_{\mathrm{APMarkov}} + P_{\mathrm{IS}} + \mathrm{EP} + \Delta M \right), \qquad (8)$$

where $\sum P_{\mathrm{APMarkov}}$ denotes the sum of the probability of APs and the APs contain the vul, and P_{IS} denotes the probability of the Interdiction Surface, which is defined as

$$P_{\mathrm{IS}} = 1 - \prod_{m \in \mathrm{IS}} [1 - \mathrm{EP}(m)], \qquad (9)$$

and ΔM represents the changes of three AP-based metrics, which is defined as

$$\Delta M = 0.33 \times \left(\Delta \mathrm{Num}_{\mathrm{APs}} + \Delta \mathrm{Exp}_{\mathrm{APlen}} - \Delta \mathrm{Len}_{\mathrm{SAP}} \right), \qquad (10)$$

where $\Delta \mathrm{Num}_{\mathrm{APs}}$ denotes the changes of the number of APs, $\Delta \mathrm{Exp}_{\mathrm{APlen}}$ denotes the changes of the expectation of AP lengths, and $\Delta \mathrm{Len}_{\mathrm{SAP}}$ denotes the changes of the shortest AP. Note that the values of changes of three AP-based metric are normalized to adapt for the accumulated probability in Equation (8).

The main procedure for the composite metric calculation is shown in a flow chart (Figure 4). It combines the results obtained in the first two phases. The proposed system security metric for a given ICS is the sum of each composite metric calculated after each vulnerability remediation. After all APs are eliminated with the removal of the last edge in the selected Interdiction Surface, the ΔM cannot be calculated. Hence, the loop-out condition in Figure 4 is that there is only one edge in the Interdiction Surface.

According to Figure 4, the results of the motivating example are $\mathrm{Com\_metric}(S_0 \longrightarrow S_2) = 0.67$ and $\mathrm{Com\_metric}(S_1 \longrightarrow S_4) = 0.42$, respectively. The security-level value for the example system is the sum of these two values, 1.09.

5. Case Study

In this section, we validate the effectiveness of the proposed methodology with a complete and nearly realistic case. Initially, a hypothetical ICS scenario is introduced in Subsection 5.1. Then, a vulnerability-oriented AG is constructed in Subsection 5.2 to elaborate the representations of each node and each edge. In Subsection 5.3, each AP is mapped into the AMC to obtain an absorbing Markov-based state transition AG, and the probability of AP is calculated as well. Finally, the composite metric is analyzed to assess the security level in the situation of the vulnerability remediations in Subsection 5.4.

The proof-of-concept system is implemented in Python (version 3.8.10), running on an Ubuntu (version 20.04.1 LTS) Linux virtual machine assigned with the Quad-core CPUs and the 4 G RAM. All directed node-edge diagrams and all statistical figures are demonstrated, respectively, by the Graphviz (version 0.16) and the Matplotlib (version 2.2.5).

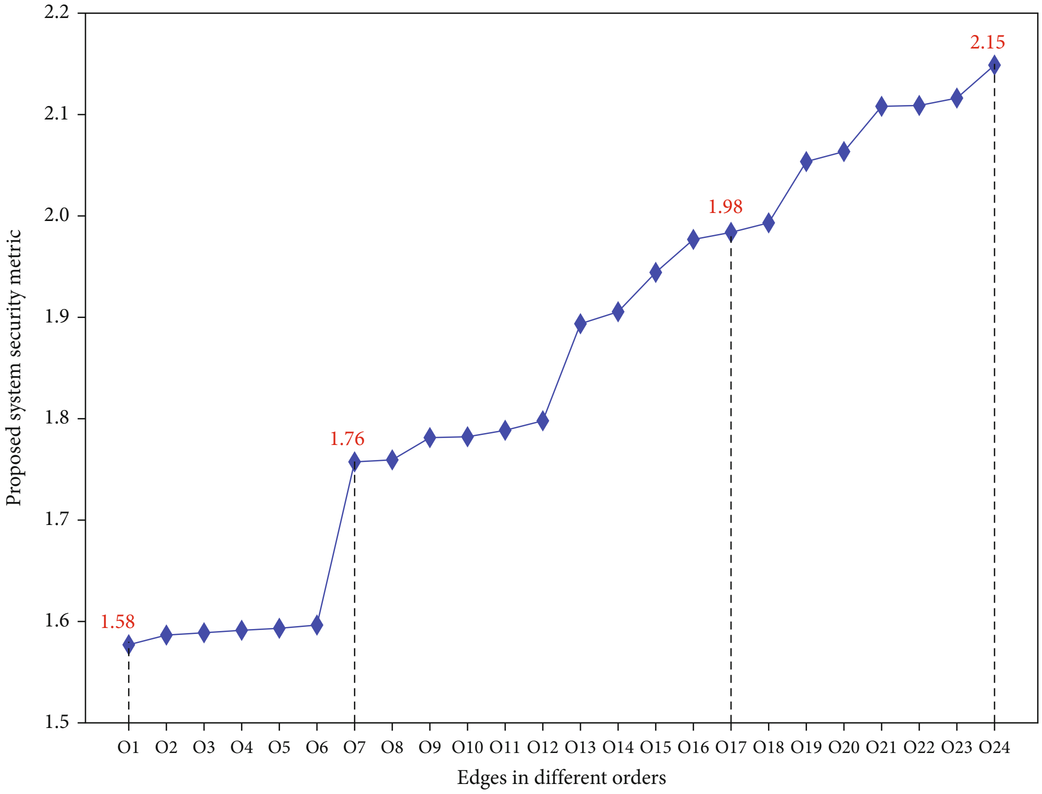


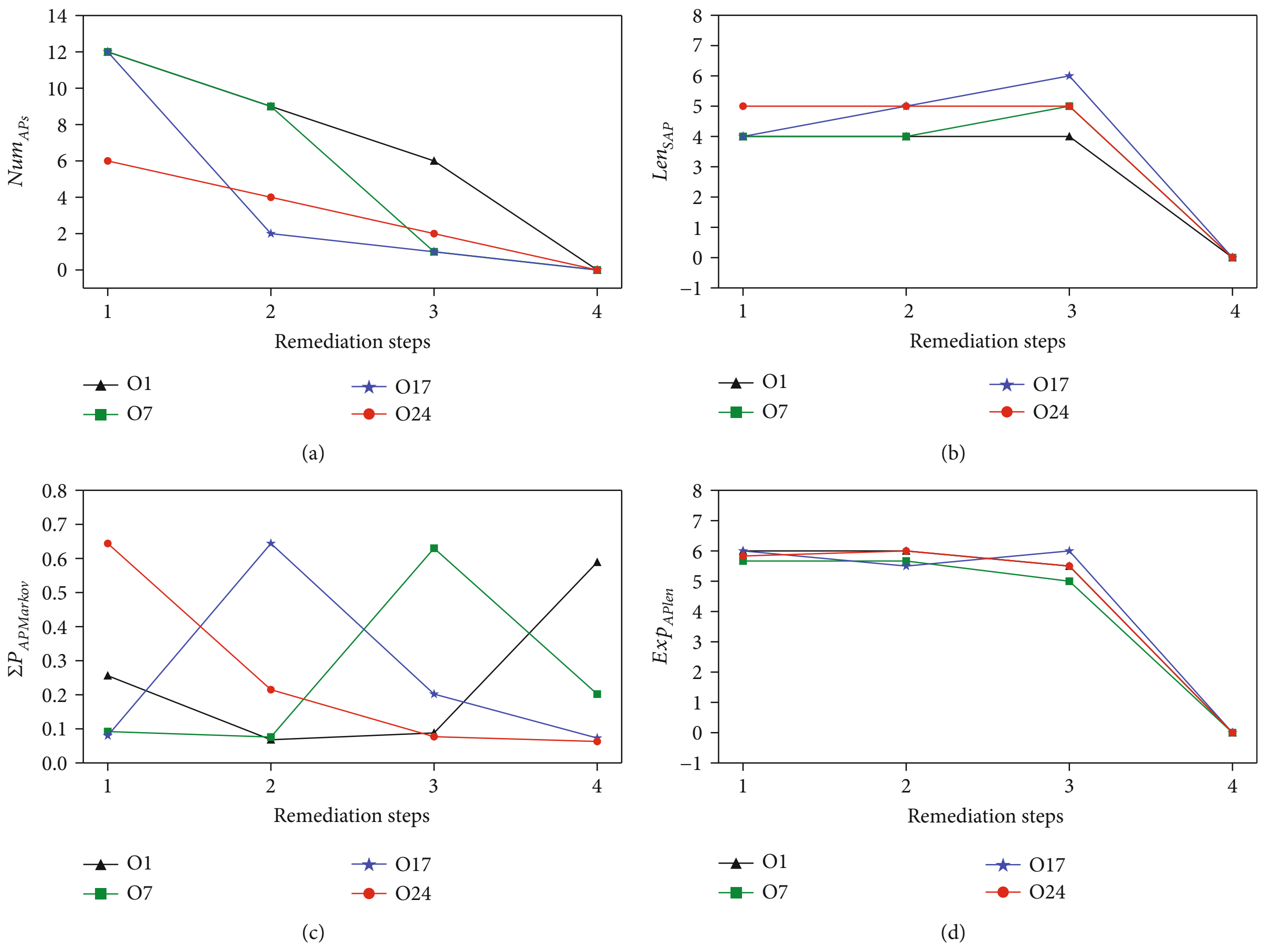
Figure 9: Proposed system security metric.

5.1. Hypothetical ICS Scenario. A hypothetical ICS scenario is illustrated in Figure 5, which is referred from the literature [29]. It shows a simplified SCADA system whose structure is in accordance with the real-world practice. The system is generally divided into three network domains. The network domain regarding the enterprise business process is omitted because it is out of our research scope. However, we assume that a compromised computer in that domain is a point of entry that is exploited by all possible multistep and multihost attacks targeting the physical process. The supervision and control network domain undertakes tasks such as an operating data acquisition and the remote monitoring on the industrial devices. Devices in this domain such as the engineering workstation (EWS) and the operation workstation (OWS) contain commercial-off-the-shell hardware and software whose known vulnerabilities could be always discovered. The production network domain is responsible for manipulating and regulating field devices by a series of networked and embedded ones such as the PLCs and the Human Machine Interface (HMI). Those devices gradually attracted the attention by attackers who aim to destroy the physical process. In this scenario, the PLCs have the master-slave architecture. We assume that the ultimate attack goal is the slave PLC.

5.2. Vulnerability-Oriented Attack Graph. A vulnerability-oriented AG for the ICS scenario is shown in Figure 6. The source node S_0 represents the compromised computer, and the terminal node T represents the slave PLC. The AG contains 11 nodes and 20 edges, which generates 16 APs terminated at the T. The construction approach for the AG is on the basis of our previously presented work [30] that focuses on an automatic planning-based AP discovery. In addition, the nodes in the graph are rearranged to demonstrate in a hierarchical way. It is convenient to test the Interdiction Surface while implementing Algorithm 1.

As listed in Table 3, the nodes in the AG represent the affected components on specific devices. Moreover, the access control relations among the components are given. The values in the last column represent the component impact, which are designated according to the response (R4) in Subsection 4.1. In particular, the impact value of the compromised computer is set to 1000 just for the purpose of the analysis. On one side, it avoids the ideal result that the Interdiction Surface only contains the edge E_1. On the other side, the optimal Interdiction Surface could be selected by properly adjusting the values of the component impact. It may be an effective way to reselect the vulnerability remediations owing to some special cases. For an example, industrial devices are unable to patch bugs in a continuous operation task.

The vulnerabilities from the National Vulnerability Database (NVD, https://nvd.nist.gov/) are assigned to the affected components disclosed in recent years. For simplicity, each component only includes one vulnerability. Each edge is related to one vulnerability encoded with a unique Common Vulnerabilities and Exposures (CVE) identification. The severity and the ES are directly searched in the CVSS by using the unique identification as an index. The information on the vulnerability is collected in Table 4.



(a)

(b)

(c)

(d)

Figure 10: Existing security metric analysis.

Especially, two different edges correspond to the same vulnerability in the table because both endpoints of each edge represent the different affected components.

5.3. Absorbing Markov Chain. An absorbing Markov-based state transition AG is illustrated in Figure 7. Each AP in Figure 6 is mapped into the AMC. The value on each edge represents the transition probability whose initial value equals EP. Except for the source node and the terminal node, each node is added an edge pointing to itself, which represents a situation that means a failure of transition to the other state. And the initial value of the edge is set to 1. Given that all transition probability for each state in the AMC should be added up to 1, the value of each edge is recalculated as shown in Figure 7. Note that the edges pointing to themselves are only involved into the calculation on the AMC. In other words, such edges only have effects on the calculation of transition probability.

In Table 5, the top 10 probabilities of AP are listed among all APs. It is observed that the value of the probability has become quite small after multiplying all the transition probabilities for the edges of the AP, as the similar method presented in [10]. Subtle differences in numerical values between two APs make it difficult to compare, let alone to assess the security level for a given system based on the single metric. Unfortunately, the metric ignores the exploitability of each vulnerability in the situation of its remediation. Take the fifth AP and the eighth AP for instance. Excluding all other factors, the probability value of the fifth AP is almost twice as much as the one of the eighth AP. However, the eighth AP contains higher severity vulnerability than the fifth AP.

5.4. Proposed Composite Metric Analysis. A total of 215 Interdiction Surfaces are discovered for the ICS scenario. The top 20 of the results are listed in Table 6. It is obvious that the optimal Interdiction Surface is the set {E2, E4, E10, E11} with the lowest score in **P1**. The lower the score is, the smaller the impact on the ICS is. Meanwhile, the effect from the vulnerability remediations is relatively optimal. For instance, both the optimal Interdiction Surface and the tenth one contain the same number of the edges. The difference lies in the combination of the edges. E10 is involved into the optimal Interdiction Surface but E20 is into the tenth one. The devices connected to E10 are OPC Server and OWS2 in the supervision and control network. The vulnerability remediations have less influence on the physical process. However, the devices connected to E20 are the master

PLC and the slave PLC. These devices directly affect the physical process while remedying the vulnerability.

In order to further demonstrate the effectiveness of prioritizing the Interdiction Surfaces, the value of three terms in Equation (3) and the final result are shown in Figure 8. 20 horizontal axis points are listed in Table 7 representing the Interdiction Surfaces. We obtain a list with prioritizing all Interdiction Surface on the basis of their results. And then, one Interdiction Surface is taken out of each ten among the list until the total number of them reaches 20. It is observed that only the curve of the score_{IS} has a monotonically increasing trend, which means that none of three terms determines in isolation to get the optimal Interdiction Surface.

In Table 8, the ranking results of the edges in the optimal Interdiction Surface and the composite metric for each vulnerability are listed as follows. The value of the system security metric for the ICS scenario is the sum of the composite metric in each step, and its result is 2.15.

The composite metric is obtained for vulnerability remediations in the context of the ICS; however, it is ought to prove whether the metric can be taken place by the AP-based security ones in the literature [6, 23, 24] or not. Part of that point has been mentioned in Subsection 4.2 by a simple example. Some more intuitive comparisons between the proposed metric and the existing ones used in isolation are shown in Figures 9 and 10.

All permutations of the edges in the optimal Interdiction Surface are obtained, 24 sequences. The proposed system metric is calculated for each sequence. According to the value of the metric, each sequence is ranked and labeled as Oj where $j = 1, 2 \cdots, 24$. As illustrated in Figure 9, the sequence with the highest value is O24 whose sequence is $\text{E4} \gg \text{E11} \gg \text{E10} \gg \text{E2}$. The sequence corresponds to the result in Table 7. We select 4 sequences that are O1, O7, O17, and O24 so as to observe the changes of the existing AP-based metrics, as illustrated in Figure 10. The four selected sequences are intentionally assigned different initial edges, and the other three edges are in random order. The value of the remediation step on the horizontal axis points is the order of the edges in these four sequences.

Obviously, it is difficult to decide which sequence is optimal by the comparison of results from the four cases of Figure 10. Recall that the shortest AP and the expectation of AP should have the similar trend to assess the security level. However, the inconsistent conclusions for O7 and O17 are drawn between case (b) and case (d). The reason why the proposed metric is comparable is that the Triangle Module Operator plays a desirable role in reconciliation while fusing the ranking results and the benefits from the basic AP-based metrics. What is worse, the existing metrics lack consideration for the component impact so that they have no capability of the system-level assessment for the ICS scenario.

6. Conclusion

In this paper, we have proposed a composite metric for the vulnerability remediations in the ICS. The proposed metric integrates the urgent security demands into the novel definition called the Interdiction Surface including the vulnerabilities that are removed to eliminating all APs. Ranking the remediations for vulnerabilities is an effective way to decrease the probability to launch the multistep and multihost attacks as soon as possible. The composite metric overcomes the shortcomings of the existing ones used in isolation, which is more reasonable to assess the security level for the ICS. The entire procedure on the basis of the AP-based analysis is not only theoretical support but also practical to implement in reality.

Our future research direction is to improve the scalability for a large-scale environment of the ICS. Note that finding out all minimum ECSs in the AG is not trivial due to the fact that it is an NP-complete problem. More related algorithms on the fast enumeration of the ECSs will be introduced to the proposed methodology. In addition, parallel computing method based on hypergraph partitioning for the AG will be explored to calculate the composite metric at the same time so as to enhance the solving efficiency. And the AP reduction strategy is attempted to avoid invalid paths that are probably infeasible to reach the goal.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

All the authors hereby declare no conflicts of interest.

Acknowledgments

Our work is supported by the National Key R&D Program of China (2021YFB2012400).

References

[1] M. M. Ahmadian, M. Shajari, and M. A. Shafiee, “Industrial control system security taxonomic framework with application to a comprehensive incidents survey,” *International Journal of Critical Infrastructure Protection*, vol. 29, article 100356, 2020.

[2] Z. C. Hu, X. Z. Yu, J. T. Shi, and L. Ye, “Abnormal event correlation and detection based on network big data analysis,” *Computers, Materials & Continua*, vol. 69, no. 1, pp. 695–711, 2021.

[3] X. F. Wang, R. Ma, D. H. Tian, and X. J. Wang, “VCPEC: vulnerability correlation analysis based on privilege escalation and Coritivity theory,” in *2020 the 10th International Conference on Communication and Network Security*, pp. 99–108, New York, NY, USA, 2020.

[4] A. Ur-Rehman, I. Gondal, J. Kamruzzaman, and A. Jolfaei, “Vulnerability modelling for hybrid industrial control system networks,” *Journal of Grid Computing*, vol. 18, no. 4, pp. 863–878, 2020.

[5] I. Stellios, P. Kotzanikolaou, and C. Grigoriadis, “Assessing IoT enabled cyber-physical attack paths against critical systems,” *Computers and Security*, vol. 107, article 102316, 2021.

[6] N. Idika and B. Bhargava, "Extending attack graph-based security metrics and aggregating their application," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 1, pp. 75–85, 2012.

[7] B. C. Che, L. Liu, and H. L. Zhang, "KNEMAG: key node estimation mechanism based on attack graph for IoT security," *Journal on Internet of Things*, vol. 2, no. 4, pp. 145–162, 2020.

[8] U. Garg, G. Sikka, and L. K. Awasthi, "Empirical analysis of attack graphs for mitigating critical paths and vulnerabilities," *Computers & Security*, vol. 77, pp. 349–359, 2018.

[9] X. G. Liu, "A network attack path prediction method using attack graph," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–8, 2020.

[10] K. Bi, D. Z. Han, G. C. Zhang, K. C. Li, and A. Castiglione, "K maximum probability attack paths generation algorithm for target nodes in networked systems," *International Journal of Information Security*, vol. 20, no. 4, pp. 535–551, 2021.

[11] H. Wang, Z. F. Chen, J. P. Zhao, X. Q. Di, and D. Liu, "A vulnerability assessment method in industrial Internet of Things based on attack graph and maximum flow," *IEEE Access*, vol. 6, pp. 8599–8609, 2018.

[12] M. Barrère, C. Hankin, N. Nicolaou, D. G. Eliades, and T. Parisini, "Measuring cyber-physical security in industrial control systems via minimum- effort attack strategies," *Journal of Information Security and Applications*, vol. 52, p. 102471, 2020.

[13] M. Barrère and C. Hankin, "Analysing mission-critical cyber-physical systems with AND/OR graphs and MaxSAT," *ACM Transactions on Cyber-Physical Systems*, vol. 5, no. 3, pp. 1–29, 2021.

[14] B. Yiğit, G. Gür, F. Alagöz, and B. Tellenbach, "Cost-aware securing of IoT systems using attack graphs," *Ad Hoc Networks*, vol. 86, pp. 23–35, 2019.

[15] G. Stergiopoulos, P. Dedousis, and D. Gritzalis, "Automatic analysis of attack graphs for risk mitigation and prioritization on large-scale and complex networks in Industry 4.0," *International Journal of Information Security*, vol. 21, no. 1, pp. 37–59, 2022.

[16] P. Mell, J. Shook, and R. Harang, "Measuring and improving the effectiveness of defense-in-depth postures," in *Proceedings of the 2nd Annual Industrial Control System Security Workshop on - ICSS '16*, pp. 15–22, Los Angeles, CA, USA, 2016.

[17] A. T. Al Ghazo and R. Kumar, "Identification of critical-attacks set in an attack-graph," in *2019 IEEE 10th annual ubiquitous computing, Electronics & Mobile Communication Conference (UEMCON)*, pp. 0716–0722, New York, NY, USA, 2019.

[18] G. George and S. M. Thampi, "Vulnerability-based risk assessment and mitigation strategies for edge devices in the Internet of Things," *Pervasive and Mobile Computing*, vol. 59, article 101068, 2019.

[19] G. George and S. M. Thampi, "Combinatorial analysis for securing IoT-assisted Industry 4.0 applications from vulnerability-based attacks," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 1, pp. 3–15, 2022.

[20] G. Cybenko and G. F. Stocco, "Asymptotic behavior of attack graph games," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, pp. 104–112, Springer International Publishing, 2018.

[21] A. Ben Yaghlane, M. N. Azaiez, and M. Mrad, "System survivability in the context of interdiction networks," *Reliability Engineering and System Safety*, vol. 185, pp. 362–371, 2019.

[22] M. Mrad, U. S. Suryahatmaja, A. Ben Yaghlane, and M. N. Azaiez, "Optimalk cut-setsin attack/defense strategies on networks," *IEEE Access*, vol. 8, pp. 131165–131177, 2020.

[23] M. Pendleton, R. Garcia-Lebron, J. H. Cho, and S. Xu, "A survey on systems security metrics," *ACM Computing Surveys*, vol. 49, no. 4, 2017.

[24] H. Hu, Y. L. Liu, H. Q. Zhang, and Y. C. Zhang, "Security metric methods for network multistep attacks using AMC and big data correlation analysis," *Security and Communication Networks*, vol. 2018, 14 pages, 2018.

[25] C. Shan, B. Jiang, J. Xue, F. Guan, and N. Xiao, "An approach for internal network security metric based on attack probability," *Security and Communication Networks*, vol. 2018, Article ID 3652170, 11 pages, 2018.

[26] P. Mukherjee and C. Mazumdar, "'Security concern' as a metric for enterprise business processes," *IEEE Systems Journal*, vol. 13, no. 4, pp. 4015–4026, 2019.

[27] Y. C. Zhao, Y. B. Che, T. J. Lin et al., "Minimal cut sets-based reliability evaluation of the more electric aircraft power system," *Mathematical Problems in Engineering*, vol. 2018, Article ID 9461823, 11 pages, 2018.

[28] Y. N. Cao and M. Q. Wu, "RPL based on triangle module operator for AMI networks," *China Communications*, vol. 15, no. 5, pp. 162–172, 2018.

[29] A. Abou el Kalam, "Securing SCADA and critical industrial systems: from needs to security mechanisms," *International Journal of Critical Infrastructure Protection*, vol. 32, article 100394, 2021.

[30] Z. B. Wang, Y. F. Zhang, Z. Y. Liu, X. J. Wei, Y. L. Chen, and B. Wang, "An automatic planning-based attack path discovery approach from IT to OT networks," *Security and Communication Networks*, vol. 2021, Article ID 1444182, 18 pages, 2021.