2021

Criticality Based Optimal Cyber Defense Remediation in Energy Delivery Systems

Kamrul Hasan
Tennessee State University

Sachin Shetty
Old Dominion University, sshetty@odu.edu

Md. Sharif Ullah
Old Dominion University

Amin Hassanzadeh
Cyber Fusion Center

Tariqul Islam
Syracuse University

Original Publication Citation

Hasan, K., Shetty, S., Ullah, M., Hassanzadeh, A., & Islam, T. (2021). Criticality based optimal cyber defense remediation in energy delivery systems. *EAI Endorsed Transactions on Security and Safety*, *8*(28), 170949. https://doi.org/10.4108/eai.10-9-2021.170949

EAI Endorsed Transactions
on Security and Safety
Research Article EAI.EU

Criticality based Optimal Cyber Defense Remediation in Energy Delivery Systems

Kamrul Hasan[1], Sachin Shetty[2], Md. Sharif Ullah[2], Amin Hassanzadeh[3], Tariqul Islam[4,*]

[1]Tennessee State University, Nashville, TN, USA
[2]Old Dominion University, Norfolk, VA, USA
[3]Accenture Labs, Cyber Fusion Center, Accenture
[4]Syracuse University, Syracuse, NY, USA

Abstract

A prioritized cyber defense remediation plan is critical for effective risk management in Energy Delivery System (EDS). Due to the complexity of EDS in terms of heterogeneous nature blending Information Technology (IT) and Operation Technology (OT) and Industrial Control System (ICS), scale and critical processes tasks, prioritized remediations should be applied gradually to protect critical assets. In this work, we propose a methodology for a prioritized cyber risk remediation plan by detecting and evaluating paths to critical nodes in EDS. We propose critical nodes characteristics evaluation based on nodes' architectural positions, a measure of centrality based on nodes' connectivity and frequency of network traffic, as well as the controlled amount of physical loads. The paper also examines the relationship between cost models of budget allocation for the removal of vulnerabilities on critical nodes and its impact on gradual readiness.

Received on 15 June 2021; accepted on 01 September 2021; published on 10 September 2021

Keywords: Cyber defense, Criticality, Energy Delivery Systems, Attack graph, Cost models

doi:10.4108/eai.10-9-2021.170949

1. Introduction

The integration of Information Technology (IT) and Operational Technology (OT) in Cyber-Physical Systems (CPS) has resulted in increased efficiency and facilitated real-time information acquisition, processing, and decision making. However, the increase in automation technology and the use of the internet for connecting, remote controlling, and supervising systems and facilities has also increased the likelihood of cybersecurity threats that can impact safety of humans and property[1]. There is a need to assess cybersecurity risks in the power grid, nuclear plants, chemical factories, etc. to gain insight into the likelihood of safety hazards. Quantitative cybersecurity risk assessment will lead to informed cyber defense remediation and will ensure the presence of a mitigation plan to prevent safety hazards. In this work, using Energy Delivery Systems (EDS) as a use case to contextualize a CPS, we address key research challenges in managing cyber risk for cyber defense remediation.

EDS is complex in their physical architecture, in the cyber infrastructure that controls them, and the supported business processes[2]. There is a need to understand how cyber threats may be manifested and focus on assessing the impact of the EDS operation under threat. There is also a need to prioritize mitigation plans, by focusing on critical assets in EDS while maintaining acceptable performance levels during production.

Proposed measure of nodes' criticality for risk analysis in EDS[2][3][4] typically ignore either the heterogeneous nature of nodes as well as the interdependence between IT and OT.

In this paper, a heterogeneous network refers to interconnected IT and OT network including computers and control devices with different operating systems, firmware, protocols, and services.

For example, the U.S. 2003 blackout[2] was initiated to a large extent by the failure that initially occurred

*Corresponding authors. Email:
mhasan1@tnstate.edu, sshetty@odu.edu, mulla001@odu.edu, amin.hassanzadeh@accenture.com, mtislam@syr.edu

in the IT component and resulted in the failure of an OT component. Several studies also advocate[5][6] considering network flows to model a node's criticality considering the node's heterogeneity. However, the model has been evaluated either for an IT or for an OT system separately.

Researchers have analyzed system risk in the context of cyber attack using attack graph[7] without factoring in node criticality. *Here, the criticality of a node indicates the maximum amount of damages inflicted on the system when an attacker has compromised the node*. The notion of node critically was defined by[8][9] employing attack graph of an IT infrastructure based on pre and post association with other nodes. The criticality of a node increases with associations with neighboring nodes. In the realm of data-driven cyber risk analysis, Rezvani et al.[5] developed a flow based architecture to model cyber risk and Zhang et al.[6] developed a model for fast node ranking in a scalable network leading to fast convergence.

Price et al.[3] proposed a model to calculate nodes' criticality for ICS risk based on network connectivity alone. Researchers have also proposed heuristic based resource optimization scheme to manage risk effectively [8] [7][10][11][12]. In this work, we address heterogeneous IT/OT networks while modeling node criticality which is relevant in ICS environments. Some of the aforementioned efforts factor node criticality in either IT or OT environments alone and assume homogeneous network, wherein all nodes operates in a similar manner and configured with the same operating system (OS), and uses the same network protocols.

In this work, we incorporate impacts of heterogeneous networks in modeling data-driven node criticality for EDS. We also propose resource allocation methods characterized with fast convergence to manage the cyber risk effectively. The main contributions of this work are summarized as follows:

1. Model criticality of a node in the EDS infrastructure considering node heterogeneity.

2. Propose an optimal resource allocation (remediation) scheme of a fixed resource budget according to nodes' criticality that minimizes the network risk.

3. Empirical validation within an ICS testbed to assess performance of the criticality model and resource allocation scheme.

The rest of the paper is organized as: in Section II, we discuss the system model includes modeling criticality of nodes, determining critical paths and resource optimization to reduce risk. In Section III, the implementation of EDS in ICS test-bed to collect network's logs, hosts' logs, and protocol traces to validate our models and then result analysis. Finally, we conclude in Section IV.

2. System Model

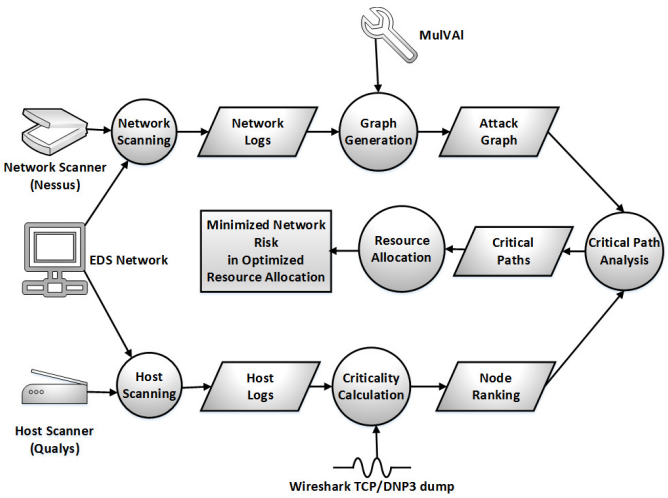

Figure 1. System Model

Fig. 1 depicts the processes and interactions among different modules in the proposed risk analysis and resource allocation model. *Here, resource refers to the deployable items to mitigate exploiting a vulnerability in a system that can be converted to monetary value like man hour for installing new patches, related system down time cost, and new patch purchased cost*. Leveraging network scanning data and host logs, such as TCP/DNP3 dump, the system creates Attack Graph (AG) using[13] to determine nodes' criticality. The risk analysis module calculates the risk of exploiting a vulnerability of a node in attack graph as a product of the probability of exploiting the vulnerability and potential damages occur from acquiring the node. The damage is quantified from node criticality for the target EDS. After calculating node's risk, the security administrator can filter out the most critical paths and can reduce risk for those paths by selecting appropriate remediations. In the next subsections, we are going to discuss every module of our system.

2.1. Attack Graph Generation

The open source tool MulVal[13] is used in our system to create AG from network scanned data. The semantics of MulVal AG is taken from[7] and is best explained with an example in Fig. 3. The labels of the graph nodes are displayed at the right hand side of AG diagram. The intrinsic probability for exploiting a vulnerability without pre-conditions inside the oval shape is taken from $CVSS$ base score[7], then the cumulative probability (CP) is derived from this intrinsic probability of a vertex after following methods in [14]. There is an expected loss C_i associated with each vertex/node that represents the loss value in monetary units when the vertex has been acquired or exploited.

This loss value also indicates the *Criticality* of this node.

A dependency attack graph can be specified as a directed graph $G = (V, E, P, C)$ where V is a set of vertices (nodes) that represent pre-conditions, vulnerabilities and exploits and E is a set of edges (arcs) that represent relationships between the pre-conditions, vulnerabilities and exploits. There is an intrinsic probability p_i associated with each vertex that represents the likelihood of an attacker exploiting a vulnerability without considering the pre-conditions. There is an expected loss C_i associated with each vertex that represents the loss value in monetary units when the vertex has been acquired or exploited. The labels of the graph nodes are displayed at the right hand side of AG diagram. For simplicity, two types of vertices presented on Fig 3. A diamond vertex represents acquired privileges once an attacker successfully exploits a vulnerabilities. An elliptic vertex represents an attack step that can lead to acquiring privileges. The probability of exploiting a vulnerability is taken from CVSS base score[15][7][14], and used to derive the Conditional Probability (CP). We have considered two types of nodes in our AG; an AND and an OR node. The equations for CP of AND node and OR node are derived from [14], which are: If the execution of a node e requires two conditions c_1 and c_2 then,

$$p_{CP}(e) = p(c_1).p(c_2).p(e) \tag{1}$$

If a condition c can be satisfied by either node e_1 or node e_2 (or both) then:

$$p_{CP}(c) = p(c)(p(e_1) + p(e_2) - p(e_1).p(e_2)) \tag{2}$$

2.2. Host Scanning and Criticality calculation

The criticality of a node in an EDS depends on many factors. To model the criticality of a node in EDS, we primarily focus on three factors[16][17]:

$$C(i) = \alpha l(i) + \beta CEN(i) + \gamma d(i) \tag{3}$$

where $C(i)$ is the criticality of the node i, driven by three properties $l(i)$, $CEN(i)$, and $d(i)$ respectively indicate locality, centrality and physical damage properties of critical node i. Each characteristic has a tuning parameter α, β, and γ for administrator's adjustments usages to control relative importance of three characteristics. As an example, in OT networks, γ should have more weight to consider physical damage, whereas in control system, β should be increased to consider centralized control nodes more.

Locality (l): locality is defined as relative position of a node according to network layers defined in IEC 62443 standard[18] for EDS. Servers closer to physical assets are considered to be more cyber critical and receive higher value. For example, in an EDS shown in Fig. 2, Supervisory Control And Data Acquisition 1 (SCADA1) and SCADA2 servers located at level 2 or 3 are more critical than workstations located at level 4 or 5. As such, a higher score assigned to an asset indicates that it is closer to the physical processes. The localization of a node is mapped from running services and processes in the node which are collected from hosts' scan logs.

Centrality (CEN) : is a measure of criticality within the same layer of the IEC 62443 model. Since nodes at the same layer may have different attack propagation opportunities, individual node criticality can vary. Quantifying relative centrality of a single layer, is done with weighted network depicting network connectivity (unique neighbor connections) and traffic load per node. The load measure is considered by enumerating the number of packets (TCP, DNP3, etc.) that are exchanged between a pair of nodes normalized by total number of packets traversing the layer during a pre-defined period of time. Unique connections count (Degree) of a node i is the number of communicated adjacent nodes in a network[19]:

$$k_i = c_d(i) = \sum_{j=1}^{N} x_{ij} \tag{4}$$

where j represents all other nodes, N is the total number of nodes, and x is the adjacency vector, in which $x_{ij} = 1$, if node i is connected to node j, and $x_{ij} = 0$ otherwise. Degree has generally been extended to the sum of weights when analyzing weighted networks[19] and labeled strength on node. Unique connections weight is formulated as follows:

$$s_i = c_d^w(i) = \sum_{j=1}^{N} w_{ij} \tag{5}$$

where, w_{ij} is defined as the weight of the link from node i to j. The product of count and weight yields the degree indicating the level of involvement of a node within its network. In addition, the tuning parameter, δ, determines the relative importance of the number of links compared to tie weights. More specifically, we propose a degree centrality measure, which is the product of the number of nodes that a focal node is connected to and the average weight to these nodes adjusted by the tuning parameter:

$$CEN(i) = k_i(\frac{s_i}{k_i})^{\delta} = (\sum_{j=1}^{N} x_{ij})^{1-\delta}(\sum_{j=1}^{N} w_{ij})^{\delta} \tag{6}$$

Damage Factor (d) : in order to address global topological properties in EDS context, we consider

potential damage at physical process level (L2 and L1) which is a function of the utilization of managed OT physical element. Utilization is a measure of applied electrical current (controlled power) over a period of time, within the permitted range. The higher the current is within the range, the more used the device is. Normally this information can be found from the exchanged DNP3 messages between SCADA server and substations' Remote Terminal Units (RTUs). RTUs periodically transmit voltage and current level to SCADA server so that SCADA can control a substation's operation. From current level, SCADA servers calculate the operational load of a substation. As such, an attack on more utilized SCADA controlled devices can create more physical damage. Damage is defined as [20]:

$$d(i) = (\frac{P_l(i)}{P_T})^{L^*-1} \tag{7}$$

where L^* indicates the value of the loading level where power flow diverges (P-V curve). SCADA server decides the value of L^* from monitored voltage and current level. $P_l(i)$ is loss of load for compromised system i and P_T indicates system's total load.

2.3. Discover Critical Path

To calculate the critical path from system administrator perspective, a product of cumulative probability (CP) of every node in AG and $Criticality$ of that node is computed. Here, *critical path is the path which creates maximum damages to the system if an attacker has chosen this path to attain his/her goal*. The most probable attack path may not necessarily always be the same as critical path. In this work, we assume that for an extremely skilled and knowledgeable attacker critical path is more preferable than most probable path.

2.4. Risk Analysis

The attack graph of an EDS network provides the logical representation of attacker's lateral movements. To analyze the risk of those movements, we need to estimate the complexity of movements per stage in the creation of an AG. The complexity associated with an attack is a function of the $Criticality$ of that stage as defined above denoted as C_i, evaluated as described in the previous section, the probability of exploiting a vulnerability denoted as V_i (provided by external repositories indicating the complexity of using such vulnerability), and the probability of threat manifestation in that stage denoted as T_i. Since threat intelligence vary in time according to global threat, for our model we used an equal value for all elements, set to one. As such, the risk of a stage in AG is defined as:

$$R(i) = T_i V_i C_i \tag{8}$$

2.5. Resource Allocation/Remediation Plan

Suppose we have a resource budget, B_D, and the cost to eliminate all vulnerabilities and exploits from node i is $maxA_i$, where A_i is the actual cost invested. In which the goal is to reduce the number of pre-conditions, vulnerabilities and exploits, denoted as V_i, to zero. This implies, that the number of remaining vulnerabilities, is a function of budget allocation A_i that represents actions performed on a node to remove and remediate such vulnerabilities, for every node in AG. The target function is to allocate correct A_i to each node such that overall risk is minimized. Namely:

$$min\{R\} = \sum_{i=1}^{N} V_i(A_i)C_i \tag{9}$$

Subject to,

$$\sum_{i=1}^{N} A_i \leq B_D; \sum_{i=1}^{N} maxA_i > B_D; A_i \geq 0 \tag{10}$$

The Uniform/Random Cost Model:

The simplest strategy for risk reduction is to allocate budget randomly or uniformly amongst all nodes; that is, for a given budget B_D for all N nodes, evenly divide B_D across N nodes. Therefore, $A_i = \frac{B_D}{N}$, and the risk is computed accordingly[19]:

$$R = \sum_{i=1}^{N} V_i C_i = \sum_{i=1}^{N} (1 - A_i)\ C_i \tag{11}$$

It is our assumption that the total number of vulnerabilities cannot be reduced to zero due to limited budget allocation. The vulnerability reduction function is given by:

$$V_i(A_i) = max\{(1 - \frac{A_i}{maxA_i}), 0\} \tag{12}$$

In this case we assumed a linear decline in vulnerability exploitation with increase in budget and security actions allocation.

The simplest strategy for risk reduction is to allocate resources randomly or uniformly among all nodes; that is, for the given budget B_D, evenly divide B_D across N nodes. Therefore, $A_i = \frac{B_D}{N}$, and the risk is reduced accordingly:

$$R = \sum_{i=1}^{N} V_i C_i = \sum_{i=1}^{N} \left(1 - \frac{B_D}{N}\right) C_i \tag{13}$$

It is not reasonable to allocate more than $maxA_i$ to a node, so vulnerability can not be reduced below zero.

In that case the vulnerability reduction function is:

$$V_i(A_i) = max\{(1 - \frac{\frac{B_D}{N}}{maxA_i}), 0\} \quad (14)$$

In this case, we assumed a linear decline in vulnerability exploitation with increase in resource allocation. We also assumed that uniform allocation across all nodes yields the best return on investment, B_D, and a significant reduction in the risk is the result.

The Linear Cost Model: What will be the risk reduction amount if we allocate more resources to critical nodes and less resources to less critical nodes? The disproportionate amount of budget B_D allocation to critical nodes and a smaller amount to less critical nodes to reduce overall system risk is known as linear cost model of risk reduction.
In linear cost model, the more funds allocated to A_i to protect node i, the less vulnerable is the node up to a maximum investment, $maxA_i$, as follows[19]:

$$V_i(A_i) = 1 - \sigma_i A_i; 0 \leq A_i \leq maxA_i \quad (15)$$

Here, σ_i = slope of straight line such that $0 = 1 - \sigma_i maxA_i$. The slope is determined by the cost of 100% hardening, which is $maxA_i$. Vulnerability is driven to zero when, $A_i = maxA_i$, so $\sigma_i = \frac{1}{maxA_i}$. This leads to the simple linear cost model of risk reduction:

$$min\{R(A)\} = min \sum_{i=1}^{N} C_i max\{(1 - \frac{A_i}{maxA_i}), 0\} \quad (16)$$

Subject to,

$$\sum_{i=1}^{N} A_i \leq B_D; A_i \geq 0 \quad (17)$$

To calculate the actual optimized budget allocation to each node, we need to know the $maxA_i$ for each node. According to[21] the maximum spending for hardening an asset from cyber attack should not be more than 37% of its criticality value irrespective of Exponential Power Class type attack or Proportional Hazard Class type attack. In our system model, we first determined the $maxA$ based on the most critical node[21]. Next other nodes' $maxA$ is determined by sorting the list of nodes according to their consequence values, where i enumerates nodes in ascending order by the product, C_i and $maxA_i$:

$$C_{i1} maxA_{i1} \geq C_{i2} maxA_{i2} \geq .... \geq C_{iN} maxA_{iN} \quad (18)$$

Next, allocate $maxA_{i1}$to the highest, $maxA_{i2}$ to the next highest, and so on, until the remaining budget is less than $maxA_{ik}$. The remaining budget Φ is allocated to the k^{th} ranked node, and zero is allocated to all remaining nodes. In this way, the nodes use resources in the most efficient manner are given highest priority and highest amount possible.

The ranked-order allocation strategy is optimal because it efficiently reduces the risk contribution of the highest risk nodes first, until the budget is depleted. Thus, the ranked-order allocation maintains the rank-order property established by consequences:

$$C_{i1} \frac{maxA_{i1}}{maxA_{i1}} \geq C_{i2} \frac{maxA_{i2}}{maxA_{i2}} \geq .. \geq C_{ik} \frac{\Phi}{maxA_{ik}} \geq 0$$

$$C_{i1} \geq C_{i2} \geq .. \geq C_{ik} \frac{\Phi}{maxA_{ik}} \geq 0; \frac{\Phi}{maxA_k} < 1$$

The exponential cost model: The linear cost model is unrealistic because it assumes that the vulnerability will be zero with the increased budget allocation. But in reality the vulnerability attached to a node cannot be zero since the vulnerability landscape evolves and continiously generates new threats. In other words, vulnerability reduction may suffer from diminishing returns. For this reason, researchers prefer exponential cost model[19]. The exponential cost model is exactly the same as the linear cost model except for the relationship between budget allocation and vulnerability reduction. Moreover, the allocation strategy is the same; the higher-ranked ($\frac{C_i}{maxA_i}$) nodes receive more resources than lower-ranked nodes.

The exponential cost model differs from the linear model in two important ways: (1) the actual resource allocations A_i are different, and (2) network risk is typically higher because an infinite investment is required to eliminate vulnerability entirely. A simple exponential function for vulnerability reduction is[19]:

$$V_i(A_i) = e^{-\sigma_i A_i}; 0 \leq V_i(A_i) \leq 1 \quad (19)$$

Clearly, this function asymptotically declines to zero when an infinite budget allocation is assigned to this node. Unlike the linear strategy, the exponential cost allocation never completely removes vulnerability. Allocation of budget B_D to nodes is optimized when objective function R is minimized, with budgetary constraint. The optimized function is[19]:

$$R(A) = \sum_{i=1}^{N} e^{-\sigma_i A_i} C_i - \lambda[\sum_{i=1}^{N} A_i - B_D] \quad (20)$$

where,

$$A_i = \frac{ln(\sigma_i C_i) - ln(\lambda)}{\sigma_i} \text{ and } ln(\lambda) = \frac{\sum_{i=1}^{N} \frac{ln(\sigma_i C_i)}{\sigma_i} - B_D}{\sum_{i=1}^{N} \frac{1}{\sigma_i}}$$

In this work, we kept maximum budget allocations for every node was as same as the maximum allocation for the most critical node which was ($maxA_{i1}$).

3. Implementation, Result, and Analysis:

EDS Network Implementation: We implemented an EDS network that is shown in Fig. 2 in Accenture ICS research test-bed[18]. The entire test-bed is connected to a network switch and a router, and the zoning is implemented using VLAN and firewall rules. Nodes are connected as point to point, and nodes are connected by cable instead of wireless. There are five subnets created by an external and internal firewall. The IT Workstations (WSs) were located at the IT subnet. A Web Server (WebS) is located at the DMZ subnet and is directly accessible from the Internet through external firewall. SCADA servers (L3/L2), RTUs (L1) are in different subnets under larger OT subnet that holds critical communication. The SCADA1 servers and SCADA2 servers are only accessible from the WebS of the DMZ zone. The WebS is accessible from user WS and other hosts from level 4 or 5. The user subnet contains user's WS. The firewalls allow all out-bound traffic from users subnet. The test-bed also includes Intrusion Detection System (IDS) running both IT and OT specific rules, and a commercial OT Asset Discovery and Management (ADM). They are both connected to the span port of the switch to be able to inspect the entire ICS traffic. The DNP3/TCP dump is also collected from this switch. For the purpose of simulation, we injected vulnerabilities on the test-bed machines. The user workstations contained the vulnerability CVE-2009-1918 in Internet Explorer (IE). If a user accesses malicious content using the vulnerable IE browser, the machine may be compromised. The web server (DMZ) contained the vulnerability CVE-2006-3747 in the Apache HTTP service which can result in a remote attacker executing arbitrary code on the machine. The SCADA1 and SCADA2 server contained the vulnerability CVE-2018-5313 which could allow privilege escalation up to administrator level. The SCADA1 server controls 10 RTUs of substation 1 whereas SCADA2 server controls 7 RTUs of substation 2. We assume that, if an attacker acquire the control over the SCADAs, the RTUs can be acquired as well.

Result and Analysis: The Nessus's scanned data, Qualys's host scanned logs and Wireshark's passive traces were collected from the test-bed synchronously for half an hour. An AG was created using MulVAL as depicted in Fig. 3. This AG contained logical attack paths for attacker, the the conditional probability (from Eq. 1 and Eq. 2) of exploiting vulnerabilities starting from a vantage point (internet) to a target (SCADA1/SCADA2), the relevant consequences for exploiting the vulnerability, and the risk of each exploitation.

The weighted graph is calculated from TCP/DNP3 dump data (Table 1) is shown in Fig. 4. Total exchanged packets during the half an hour time was 8006.

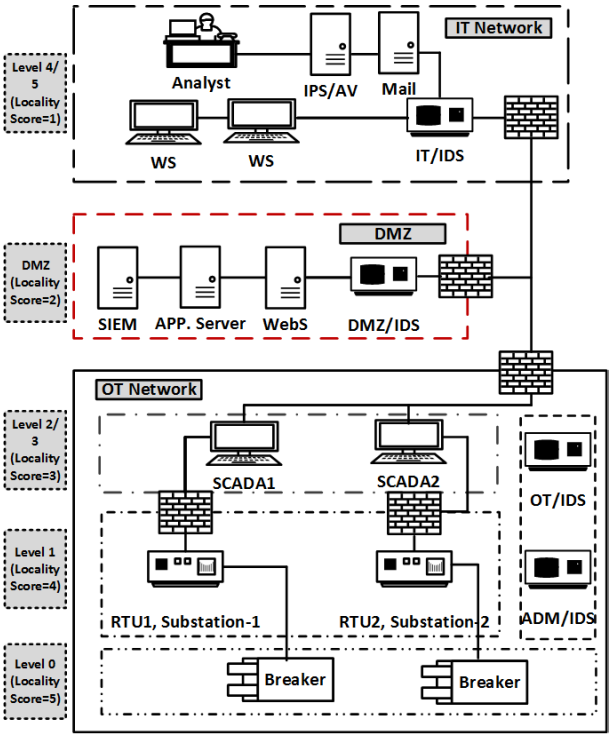

Figure 2. Logical view of EDS Test-bed

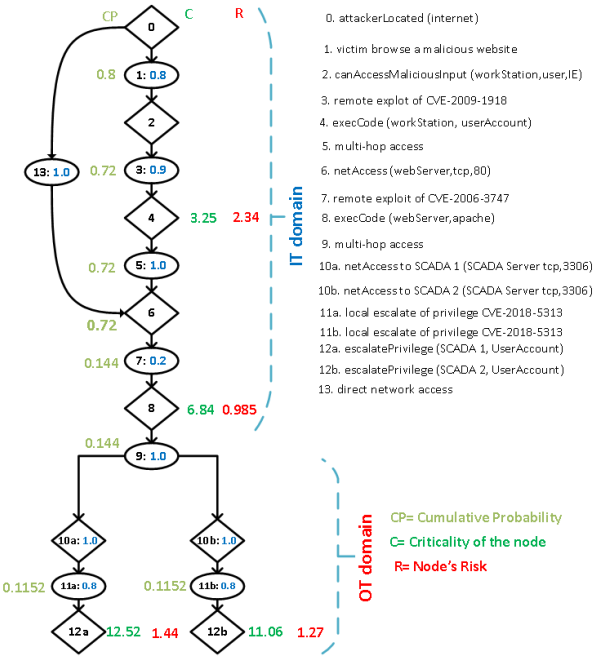

Figure 3. The AG of test-bed based EDS

The weights were calculated by dividing exchanged packets between pairs with the total numbers of packet exchanged during the time period among nodes (Table 2).

Subsequently, the centrality of criticality was calculated by plugging the Centrality presented in Fig. 4 and

Table 1. Adjacent matrix with bytes.

Total Packets=8006	WS	WebS	SCADA1	SCADA2	RTU1	RTU2
WS	0	1001	0	0	0	0
WebS	1001	0	600	400	0	0
SCADA1	0	600	0	0	1201	0
SCADA2	0	400	0	0	0	801
RTU1	0	0	1201	0	0	0
RTU2	0	0	0	801	0	0

Table 2. Weighted Adjacent Matrix

Total Packets=8006	WS	WebS	SCADA1	SCADA2	RTU1	RTU2
WS	0	0.125	0	0	0	0
WebS	0.125	0	0.075	0.05	0	0
SCADA1	0	0.075	0	0	0.15	0
SCADA2	0	0.05	0	0	0	0.10
RTU1	0	0	0.15	0	0	0
RTU2	0	0	0	0.1	0	0

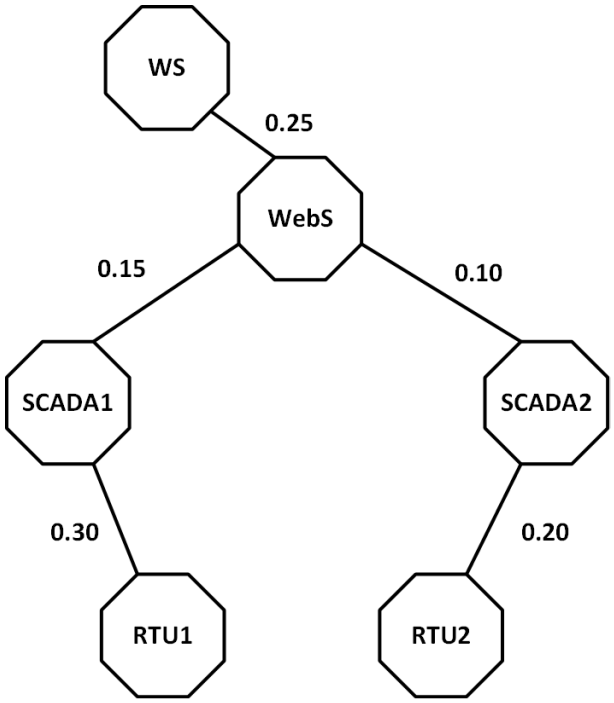

Figure 4. The weighted graph

calculated in Eq. 6. The details are shown in Table 3 for different values of δ.

Table 3 illustrates the effect of the δ on the degree of centrality for the nodes in Fig 4. It can be explained logically from this table that when $\delta = 1$ the measure's value is equal to the node's weight (Eq. 6). When $\delta < 1$ and the total node weight is fixed, the number of connections over which the weight is distributed increases the value of the measure. For example, when $\delta = 0.5$, node WebS attains a higher score than node SCADA1, despite having almost same node weight . Conversely, when $\delta > 1$ and the total node weight is fixed, the number of connections of which the weight is distributed decreases the value of the measure in favor of a greater concentration of node weight. Hence, node WebS attains almost same value of the measure than node SCADA1. So, logically in our EDS model, we choose the tuning parameter as $0 < \delta < 1$.

Locality of criticality (l) is determined from the running applications (like HMI tick), services (Operation-critical or Non-critical services, etc.), and processes collected from hosts' logs. To calculate the Damage characteristic, we only focus on the messages that regulate the level 0 sensors and breakers. From DNP3 messages, we determined that the SCADA1 is controlling a substation of 3 MW load through 10 RTUs, whereas the SCADA2 is controlling 2 MW substation through 7 RTUs. Plugging those load values in Eq. 7, we determined the Damage characteristic of criticality for individual SCADA. The

Table 3. Degree centrality at different δ.

Node	c_d	c_d^w	$CEN(i) = k_i^{1-\delta} \times s_i^{\delta}$ when $\delta =$			
			0	0.5	1.0	1.5
WS	1	0.25	1	0.5	0.25	0.125
WebS	3	0.5	3	1.225	0.5	0.204
SCADA1	2	0.45	2	0.949	0.45	0.213
SCADA2	2	0.3	2	0.775	0.3	0.116
RTU1	1	0.3	1	0.548	0.3	0.164
RTU2	1	0.2	1	0.447	0.2	0.089

individual RTU's Damage Characteristic of criticality is calculated dividing respective SCADA's Damage characteristic of criticality by the number of RTUs under this SCADA. Here, $P_T = 5MW$ and $L = 2$. As such, total criticality of a node in EDS was calculated after plugging the criticality of Locality (l), criticality of Centrality (CEN) from Table 3 and criticality of Damage (d) in Eq. 7. Table 4 shows the calculation of total Criticality (C) of individual node in EDS:

Table 4. Total Criticality Calculation

Nodes	l	CEN($\delta = 0.5$))	d	C
WS	1	0.5	0	0.325
WebS	2	1.225	0	0.684
SCADA1	3	0.949	0.6	1.252
SCADA2	3	0.775	0.4	1.106
RTU1	4	0.548	0.06	1.18
RTU2	4	0.447	0.057	1.101

For total criticality calculation in Table 4, we set $\alpha = 0.15, \beta = 0.25$ and $\gamma = 0.6$. The system administrator now can apply nodes' criticality to the AG and can determine the most critical path along with most probable paths for a certain attacker goal to achieve.

Fig. 3 also shows cumulative probability and its consequences. Assuming the attacker goal is SCADA1/SCADA2, we can see that there are two paths for the attacker to reach any of the these servers. Among those paths:$0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \rightarrow 8 \rightarrow 9 \rightarrow 10a \rightarrow 11a \rightarrow 12a; 0 \rightarrow 13 \rightarrow 6 \rightarrow 7 \rightarrow 8 \rightarrow 9 \rightarrow 10a \rightarrow 11a \rightarrow 12a$ belongs to SCADA1 and $0 \rightarrow 1 \rightarrow 2 \rightarrow 3 \rightarrow 4 \rightarrow 5 \rightarrow 6 \rightarrow 7 \rightarrow 8 \rightarrow 9 \rightarrow 10b \rightarrow 11b \rightarrow 12b; 0 \rightarrow 13 \rightarrow 6 \rightarrow 7 \rightarrow 8 \rightarrow 9 \rightarrow 10b \rightarrow 11b \rightarrow 12b$ belongs to SACDA2.

Although these two paths have the same exploitation probability from attacker starting node to the server goals of SCADA1/SCADA2, the damage that occur along the paths is not the same. Consequently, assuming that the SCADA1/SCADA2 are not the only goal, and assuming the attacker has time to analyze options, and not react to the next achievable stage of the AG during an actual attack, a knowledgeable attacker may selects the path where he/she can make the most damage. Regardless, a cyber resilient organization, prior to an attack, will harden the most impactful path prior to an attack in order to reduce the overall potential damage while protecting the golden target. So, the recommendation should be first to harden the attack path with the highest risk score.

Consequently, the system's security planner needs to propose remediations to potential paths in order to block future malicious activities. In our model, we considered the allocated operating budget as means to monetize different security actions to be performed on our network. We considered that the monetary value of every unit of criticality and resource budget can be decided by security planner respectively. Total criticality is also scaled up here from $[0 \rightarrow 2]$ to $[0 \rightarrow 20]$ for simplicity. Suppose the system planner is given 15 units of such budget. The system administrator has three options to spend the budget optimally amongst nodes:

1) allocate randomly/uniformly, 2) allocate according to the linear cost model, and 3) allocate according to exponential cost model.

Initially, before applying any operating budget as remediation, the total risk value of the network is 8.62. ($R = [(3.25 \times 0.72) + (6.84 \times 0.144) + (12.52 \times 0.1152) + (11.06 \times 0.1152) + (11.18 \times 0.1152 + (11.01 \times 0.1152)] = 8.62$). When the security administrator allocates the 15 units budget randomly/uniformly according to Eqs. 11-14, then risk reduces to 4.24 which is 49% of total risk. Yet, random/uniform allocation reduces the amount of risk irrespective of nodes' criticality and asset value, does not ensure optimize resource utilization.

Applying linear cost model after following Eqs. 15-18, the risk reduces to 4.30 which is 49.86% of total risk. The details are in Table 5:

Table 5. Linear Cost Resource Allocation

Nodes	C	$maxA$	$\frac{C}{maxA}$	A	$V(\%)$	R
WS	3.25	4.64	0.70	0	72	2.34
WebS	6.84	4.64	1.474	0	14.4	0.985
SCADA1	12.52	4.64	2.70	4.64	0	0
SCADA2	11.06	4.64	2.38	4.64	0	0
RTU1	11.18	4.64	2.41	4.64	0	0
RTU2	11.01	4.64	2.37	1.08	8.83	0.973

Allocating the budget according to exponential cost model after following Eqs. 19-20, the risk reduces to 5.41 which is 62.7% of total network risk. The details of the calculation is given in Table 6:

The risk reduction by exponential cost model is slightly lower than linear cost model because the exponential model never reduces vulnerability to zero. However, for both linear and exponential cost model the optimal allocation is ensured when the budget is distributed according to the rank of nodes. Fig. 5 shows budget allocation amongst nodes for linear cost and exponential cost allocation. In both cases, the limited budget (15 units) is allocated after ranking their criticality from highest to lowest: SCADA1, RTU1, SCADA2, RTU2, WebS, and node WS.

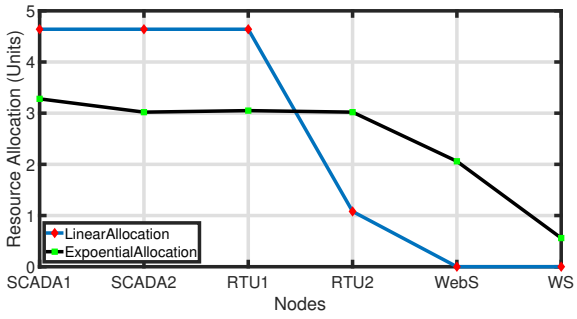

Figure 5. Linear and exponential resource allocation

Fig. 6 depicts the allocation priority- from highest to lowest. Linear and exponential allocation obeys the rank-order established by the product of $\frac{C_i}{maxA_i}$- see the columns labeled $\frac{C}{maxA}$ in Table 5 and Table 6. In fact, this property is observed in allocation strategies regardless of whether the relationship between allocation and vulnerability reduction is linear, exponential, or a power law. This establishes a hierarchy among nodes; the most critical nodes of a network are those with the highest $\frac{C}{maxA}$ value.

4. Conclusion

In this work, we presented a data-driven model to assess criticality of a node in a heterogeneous

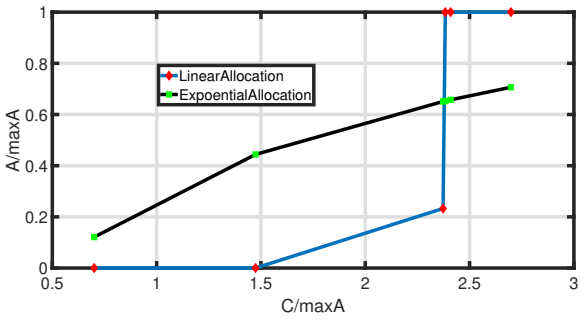

Figure 6. Linear and exponential cost allocation vs criticality

IT/OT/ICS EDS network. We also showed that assets along critical paths are as important as the target in cases of several potential attack paths can be performed. We proposed critical nodes characteristics evaluation based on architectural location in IEC 62443, measure of centrality based on nodes connectivity and frequency of network traffic, as well as controlling of electrical power. We also examined the relationship between cost models of budget allocation for removal of vulnerabilities on critical nodes and its impact on gradual readiness. Empirically validated in an actual network ICS test-bed computing nodes criticality, three cost models were examined. Although varied, we concluded the lack of correlation between types of cost models to most damageable attack path and critical nodes readiness.

References

[1] K. Hasan, "Cyber defense remediation in energy delivery systems," 2020.

[2] J. V. Milanović and W. Zhu, "Modeling of interconnected critical infrastructure systems using complex network theory," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4637–4648, 2018.

[3] P. Price, N. Leyba, M. Gondree, Z. Staples, and T. Parker, "Asset criticality in mission reconfigurable cyber systems and its contribution to key cyber terrain," in *Proceedings of the 50th Hawaii International Conference on System Sciences*, 2017.

Table 6. Exponential Cost Resource Allocation ($\lambda = 0.53$)

Nodes	C	$maxA$	$\frac{C}{maxA}$	A	$V(\%)$	R
WS	3.25	4.64	0.70	0.561	63.8	2.074
WebS	6.84	4.64	1.474	2.060	9.24	0.632
SCADA1	12.52	4.64	2.70	3.278	5.68	0.711
SCADA2	11.06	4.64	2.38	3.029	6.0	0.663
RTU1	11.18	4.64	2.41	3.051	5.97	0.667
RTU2	11.01	4.64	2.37	3.020	6.01	0.662

[4] S. Ullah, S. Shetty, and A. Hassanzadeh, "Towards modeling attacker's opportunity for improving cyber resilience in energy delivery systems," in *2018 Resilience Week (RWS)*. IEEE, 2018, pp. 100–107.

[5] M. Rezvani, V. Sekulic, A. Ignjatovic, E. Bertino, and S. Jha, "Interdependent security risk analysis of hosts and flows," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 11, pp. 2325–2339, 2015.

[6] Y. Zhang, L. Gu, X. Liao, H. Jin, D. Zeng, and B. B. Zhou, "Frank: A fast node ranking approach in large-scale networks," *IEEE Network*, vol. 31, no. 1, pp. 36–43, 2017.

[7] X. Ou and A. Singhal, *Quantitative security risk assessment of enterprise networks*. Springer, 2011.

[8] M. Alhomidi and M. Reed, "Attack graph-based risk assessment and optimisation approach," *International Journal of Network Security & Its Applications*, vol. 6, no. 3, p. 31, 2014.

[9] C. Suh-Lee and J. Jo, "Quantifying security risk by measuring network risk conditions," in *Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on*. IEEE, 2015, pp. 9–14.

[10] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of scada cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Transactions on Power Systems*, vol. 31, no. 6, pp. 4379–4394, 2016.

[11] K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem, and J. Chen, "Modeling cost of countermeasures in software defined networking-enabled energy delivery systems," in *2018 IEEE Conference on Communications and Network Security (CNS)*. IEEE, 2018, pp. 1–9.

[12] K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem *et al.*, "Self-healing cyber resilient framework for software defined networking-enabled energy delivery system," in *2018 IEEE Conference on Control Technology and Applications (CCTA)*. IEEE, 2018, pp. 1692–1697.

[13] X. Ou, S. Govindavajhala, and A. W. Appel, "Mulval: A logic-based network security analyzer." in *USENIX Security Symposium*, vol. 8. Baltimore, MD, 2005.

[14] M. Frigault, L. Wang, S. Jajodia, and A. Singhal, "Measuring the overall network security by combining cvss scores based on attack graphs and bayesian networks," in *Network Security Metrics*. Springer, 2017, pp. 1–23.

[15] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, 2006.

[16] K. Hasan, S. Shetty, S. Ullah, A. Hassanzadeh, and E. Hadar, "Towards optimal cyber defense remediation in energy delivery systems," in *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2019, pp. 1–7.

[17] K. Hasan, S. Shetty, A. Hassanzadeh, and S. Ullah, "Towards optimal cyber defense remediation in cyber physical systems by balancing operational resilience and strategic risk," in *MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM)*. IEEE, 2019, pp. 1–8.

[18] A. Hassanzadeh and R. Burkett, "Samiit: Spiral attack model in iiot mapping security alerts to attack life cycle phases," in *ICS & SCADA Cyber Security Research,2018 5th International Symposium for*. BCS, 2018, pp. 11–20.

[19] T. G. Lewis, *Network science: Theory and applications*. John Wiley & Sons, 2011.

[20] M. Touhiduzzaman, A. Hahn, and A. Srivastava, "Arcades: Analysis of risk from cyber attack against defensive strategies for power grid," *IET Cyber-Physical Systems: Theory & Applications*, 2018.

[21] S. Wang, "Optimal level and allocation of cybersecurity spending: Model and formula," 2017.