IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 1, 2018, accepted March 2, 2018, date of publication March 6, 2018, date of current version April 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2812812

A Method for Identifying Critical Elements of a Cyber-Physical System Under Data Attack

YOUPING FAN, JINGJIAO LI, AND DAI ZHANG, (Student Member, IEEE)
School of Electrical Engineering, Wuhan University, Wuhan 430072, China

Corresponding author: Youping Fan (ypfan@whu.edu.cn)

This work was supported by the National Natural Science Foundation of China under Grant 71601147.

ABSTRACT In this paper, we use hyper-network methods to identify the critical elements of a cyber-physical system (CPS) under data attack according to IEC 61850. The related works are introduced first, such as cyber offensive tools, procedures, and data attack models. Some definitions of a hypergraph are presented. Then, considering the functional attributes of logical nodes, a hyper-network model of substation auto system (SAS) is proposed using hyper-graph theory. On this basis, a CPS model that takes into account the functional influence after data attack is established. In addition, combined with the analysis of the network model, the efficiency indexes are given to evaluate the effectiveness of the CPS under data attack. The reasons why we choose these indexes in network and hyper-network model are also explained. Finally, the analysis in the case study illustrates that the method proposed is helpful for identifying critical elements of the CPS, which provides a new avenue for future vulnerability analysis research.

INDEX TERMS Cyber-physical system (CPS), critical elements identification, data attack, hyper-network model, IEC 61850.

I. INTRODUCTION

Cyber-physical systems (CPS) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core [1]. Scholars and researchers believe that the combination of CPS and power systems is an important technical basis for the development of smart grids. In addition to descriptions from the infrastructure perspective [2], [3], several studies have focused on control and communication systems and their interaction with the physical system in a smart grid [4]–[6]. Tight coupling between cyber and physical systems introduces new security concerns [2].

Several outages worldwide due to attacks on the cyber network of power systems have generated considerable recent research interest. Numerous experiments have established modeling methods and testbeds to study the security issues of CPS. Petri nets [7], the bi-level model [8], Markov games [9] and graph theory [10] have been used to model the security problems of CPS. A variety of factors, such as protection systems [11] and the attacker's total budget [8], have been considered in the modeling processes. Several prominent CPS security testbeds are listed in [12]. The smart grid security testbed at Iowa State University, named PowerCyber testbed, is comprehensive [13]. It has been used to implement and evaluate the effectiveness of attacks on several cyber targets, such as Automatic Generation Control (AGC) [14], Supervisory Control And Data Acquisition (SCADA) [15], Wide-Area Protection systems [16]. However, PowerCyber testbed has not been used for research on Substation Auto System (SAS), which is the fundamental cyber and physical component of smart grid. Markov decision process is adopted to the model cyber-physical security problem for substations in power grid considering the competition between attacker and defender [17], using a testbed built in [18]. This is useful to study the interactions between a complex power system and the Information and Communications Technology (ICT) system in a substation. A white box test based on internal structures is helpful for studying the mechanisms of offense and defense. There is still a need for a detailed modeling method of SAS according to common criteria in white box tests because implementing attacks on SAS is an effective means to affect the normal operations of power CPS. Ref. [19] proposes a cyber-physical interface matrix for reliability modeling and analyzing of modern substation protection systems based on IEC 618550, which embodies the characteristics of white box test. The definition of white box test from engineering science is contrary to black box test that can be seen only in terms of input and output without any knowledge of the internal workings. The finer-grained models are helpful to evaluate the attack profit and defense

efficiency in CPS security white box experiments. Moreover, the game process between offence and defense will always exist in a centralized or distributed CPS. Therefore, the identification of critical elements is the main task in a vulnerability assessment, which is the focus of this paper.

Reference [10] proposes a mathematical framework for cyber-physical systems and attacks from system-theoretic and graph-theoretic perspectives. Graph theory [20] and topology theory [21], [22] are usually used to evaluate vulnerability, but there are problems with applying normal graph or topology theory to CPS analysis. One is that the heterogeneity of nodes cannot be described. Another is that ''system of systems'' or ''network of networks'' is difficult to define [23]. However, ''hyper-network'' is feasible for a network which has heterogeneous nodes and is a network of networks. Hyper-networks have been used as a tool in research on supply chains [24]–[26] and intelligent decision-making [27], [28] by A. Nagurney. Additionally, hyper-networks have been used in biology [29], the Internet of Things [30], public crisis management [31], military communication networks [32], [33], air defense systems [34], and weapon system of systems [35]. In this paper, we present a novel SAS model based on hyper-network to identify the critical elements of the CPS according to IEC 61850.

Data attack is a common and direct way to cause an outage. It can be implemented in any procedure, such as data generation, communication, storage and application. Several studies have focused on data attack in CPS with respect to defense [36] and offense [37], [38]. The Markov process [39] and semi-Markov process [40] have been used to model cyber data attacks. The precondition of our research is that data attacks are assumed to be successfully implemented. Thus, attack tools, procedures and typical methods are only introduced in Section II as Related Work. The remainder of this paper is organized as follows. Section III presents some definitions of hypergragh, which are used in our work. Section IV illustrates the application of the hyper-network model to identify critical elements of a SAS according to IEC61850. Section V establishes a simple CPS model based on the model built in Section IV. The effectiveness evaluation method of a CPS under data attack is proposed, and the result analysis is provided in Section V. Finally, the conclusion and future research are proposed in Section VI.

II. RELATED WORK

A. CYBER OFFENSIVE TOOLS AND PROCEDURES

With the development of smart grid, increasingly more devices, such as IEDs, devices in ICTs and SCADA systems, are exposed to attacks by cyber offensive tools. The cyber attacks on power facilities are roughly defined as two stages: intruding target system and creating disruptive impacts [17]. However, a complete cyber attack process contains seven phases [41], which are chronologically listed in TABLE 1.

TABLE 1. Cyber attack process procedures and tools.

Num.	Attack phase	Main function	Common tools
1	Reconnaissance	Reconnaissance passively collects information on the target networks or systems. In a power system, it can be an active act sometimes, such as spying and bribing.	Websites Search engines Google Hacking WHOIS search /DNS queries Metadata Maltego
2	Scanning	Scanning aims at finding the environmental information, system type and detailed information.	Nmap Nessus OpenVAS
3	Accessing and privilege escalation	Both open source and commercial tools focus on obtaining access authorities and elevating the access authorities	Password decoding/ deciphering tool Metasploit CANVAS
4	Exfiltrating data	This process includes exfiltrating data from physical media, camouflaging data by steganography/encryption, using general protocols to enable leaving an environment, and changing the information transmission mode.	Physical exfiltrating Encryption and steganography Covert channels over general protocols Out of band (OOB) methods
5	Assaulting	Changing system configurations or environment variables, e.g. DoS attacks on specific systems or environments by constructing botnet.	Tampering of software or OS settings Attacking hardware Changing settings
6	Sustaining access	Once access authorities are successfully obtained by intruders, sustaining tools are required to continuously access the system.	Adding authorized accounts Backdoor program Adding monitor service
7	Concealing traces	This process conceals the traces of an intruder to obfuscate target systems.	Hiding physical location Modifying logs Modifying files

B. DATA ATTACK MODEL

By applying the tools listed in TABLE 1, a cyber attack can be implemented on SAS, Energy Manage System (EMS) and Market Management System (MMS) in smart grid. The data obtained by sensors in SAS are the foundation of data collection and calculations in SCADA system. SCADA telemetry data are fed into the state estimator (SE) module of EMS, where the SE module provides an estimate base power flow and network topology that is sent to the security constrained economic dispatch (SCED) module of MMS. The data in SAS resemble the information passing through the human nervous system, which helps to perceive the physical world and control behaviors. Data attacks on SAS alter the operational state and market clearing results of power system.

Attack methods are not the focus of this paper. Data attacks on SAS are classified by their effects that refer to the classifications in electronic countermeasures (ECM). According to the attack impact, an attack can be divided into a data jamming attack or a data tampering attack.

A data jamming attack seeks to make a device or network resource unavailable to users. For example, a denial of service (DoS) attack is a typical data jamming attack that is accomplished by flooding the targeted device or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled [42]. Examples of a DoS attack are Ping of Death, UDP flood, and SYN flood. A TCP-SYN Flood, for instance, is an application layer DoS attack that takes advantage of TCP protocol vulnerabilities. It sends a large number of semi-connection requests to the target server by injecting false source addresses into messages and disenabling the Three-Way Hand Shake between the target server and the node being attacked. This exhausts the target server resources and makes the server unable to answer normal connection requests. The impact of a power system under different data jamming attacks can be evaluated with building power and communication joint simulation platforms [12].

A data tampering attack is an attempt to stealthily alter data for the purpose of deceiving bad data identification modules and causing misoperations. False data injection attack (FDIA) is a typical data tampering attack that makes the user believe that the altered data reflects the real system state. Here, the user represents the control center or logical node with computing functions. FDIA is an attack on the SE function, which is proposed by Liu *et al.* [43],

$$\mathrm{z} = \mathrm{h}\left(x\right) + \mathrm{e} \tag{1}$$

where $\mathrm{z} \in \mathrm{R}^{\mathrm{m}}$ is the meter measurements vector, $\mathrm{x} \in \mathrm{R}^{\mathrm{n}}$ represents system state variables, $\mathrm{e} \in \mathrm{R}^{\mathrm{m}}$ is the Gaussian measurement noise, where $e_j \sim N\left(0, \sigma_e^2\right), j = 1, 2, \cdots, m$, and $\mathrm{h}\left(\mathrm{x}\right) = \left(\mathrm{h}_1\left(\mathrm{x}_1, \mathrm{x}_2, \cdots, \mathrm{x}_\mathrm{n}\right), \cdots, h_i\left(x_1, x_2, \cdots, x_n\right), \cdots, \mathrm{h}_\mathrm{m}\left(\mathrm{x}_1, \mathrm{x}_2, \cdots, \mathrm{x}_\mathrm{n}\right)\right)^{\mathrm{T}}$, $h_i\left(x, x_2, \cdots, x_n\right)$ is a function of $x_1, x_2, \cdots, x_n$.

A SE based on a linear DC power flow model in EMS, for example, is used to find an estimate $\hat{\mathrm{x}}$ of X, which is the best fit of the measurement z according to (2),

$$\mathrm{z} = \mathrm{Hx} + \mathrm{e} \tag{2}$$

where $H = \left(h_{i,j}\right)_{m \times n}$ [43].

If the attacker is assumed to have the ability of controlling k meters, there can be a nonzero injected attack vector $\mathrm{a} = \mathrm{Hc}$ and $\|\mathrm{a}\|_0 \leq \mathrm{k}$. According to (3), once the state vectors x and x+c are both valid in the DC power flow model, x is observationally equivalent to x+c for the control center. This implies that the injected attack vector a is unobservable and there is no detector that can distinguish x from x+c [44].

$$\mathrm{z} = \mathrm{Hx} + \mathrm{a} + \mathrm{e} = \mathrm{H}\left(\mathrm{x} + \mathrm{c}\right) + \mathrm{e} \tag{3}$$

In addition to numerous studies on the FDIA targeted at SE of a power grid, there have been studies that focus on the SE of a substation [45]–[47] and the corresponding FDIA methods [49]. Reference [48] studies the preconditions and the smallest attack cost of unobservable FDIAs on current and voltage sampling sequences from TCTR (Current Transformer) and TVTR (Voltage Transformer).

In this study, it is assumed that all the attacks on logical nodes are successful. Next, the impact on the CPS is analyzed after each logical node type fails to work properly under data attack.

III. DEFINITIONS OF A HYPERGRAPH

A. HYPERGRAPH

Reference [49] lists ten important problems in network research. One of these problems is the "network of networks", that is, the problem of interaction between heterogeneous networks. Hyper-network methods should be considered when the nodes in the network are no longer homogeneous. The hypergraph was proposed by Berge in 1970 [50]. It is the most common way to model hyper-networks and is a tool for studying the influence of the interaction between networks [51].

A hypergraph H is a pair $H = (V, E)$ where $V = \{v_1, v_2, \cdots, v_n\}$ is a finite set of vertices, and $E = \{e_1, e_2, \cdots .e_m\}$ is the set of the hypergraph's edges. e_i is an edge of the hypergraph, which is a non-empty subset of V [50], [52].

$$e_i \neq H \ (i = 1, 2, \cdots, m) \tag{4}$$

$$\bigcup_{i=1}^{m} e_i = V \tag{5}$$

B. INCIDENCE MATRIX OF THE HYPERGRAPH

A hypergraph can be represented by an incidence matrix $I\left(H\right)$. The columns in $I\left(H\right)$ correspond to the hyper-edges $e_1, e_2, \cdots .e_m$ respectively. The rows in $I\left(H\right)$ correspond to the vertices $v_1, v_2, \cdots, v_n$ respectively. The entry b_{ij} is defined in (6).

$$b_{ij} = \begin{cases} 1, & v_i \in e_j \\ 0, & v_i \notin e_j \end{cases} \tag{6}$$

C. ADJACENCY MATRIX OF THE HYPERGRAPH

If a hypergraph H is connected, its adjacency matrix $\mathrm{A}\left(H\right)$ is symmetric, non-negative and irreducible [53]. The diagonal entries of $\mathrm{A}\left(H\right)$ are zero, and the other entries are the number of hyper-edges that contain both vertices v_i and v_j. The entry a_{ij} is defined in (7) and (8).

$$a_{ij} = \begin{cases} \sum_{k=1}^{m} a_{ij}^{k}, & i \neq j \\ 0, & i = j \end{cases} \tag{7}$$

where

$$a_{ij}^{k} = \begin{cases} 1, & \text{if } v_i, \quad v_j \in E_k \\ 0, & \text{else.} \end{cases} \tag{8}$$

D. DEGREE CENTRALITY

Given a subset $S \subseteq V$, and a subset of the edge index set $J \subset \{1, 2, \cdots, m\}$, the section hypergraph H_{Sec} induced by S and J is defined as

$$H_{Sec} = \left(S, \left\{e_j \cap S \,\middle|\, j \in J, e_j \cap S \neq \emptyset\right\}\right) \tag{9}$$

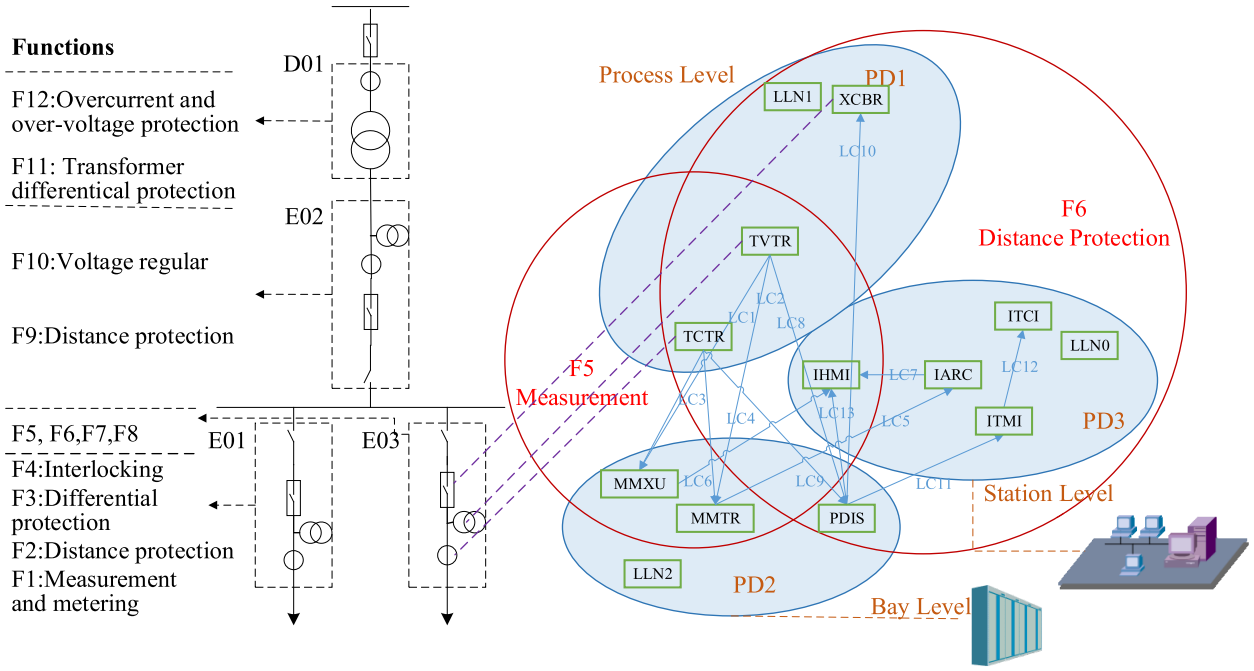

FIGURE 1. Functions of the T1-1 substation.

Given a vertex $v_i \in V$, $H_{Par}(v_i)$ is defined as a star section hypergraph of H induced by v_i and its connected edges. $C_{Degree}(i)$ is the degree of v_i, defined as the number of edges in $H_{Par}(v_i)$. It can be calculated from the incidence matrix $I(H)$.

$$C_{Degree}(i) = \sum_{j=1}^{m} b_{ij} \tag{10}$$

E. SUB-HYPERGRAPH CENTRALITY

The eigenvalues and eigenvectors of the adjacency matrix $A(H)$ help to calculate the sub-hypergraph centrality. Let $H = (V, E)$ be a simple hypergraph of order N. If $v_i \in V$, then the sub-hypergraph centrality $C_{SH}(i)$ can be expressed as:

$$C_{SH}(i) = \sum_{j=1}^{N} \left(u_{ij}\right)^2 e^{\lambda_j} \tag{11}$$

where $A(H) = UDU^T$, u_{ij} are the entries of an orthogonal matrix $U = \left(u_{ij}\right)$ whose columns are the corresponding eigenvectors to the eigenvalues λ_j, and the eigenvalues are the diagonal entries of $D = diag(\lambda_1, \lambda_2, \cdots, \lambda_N)$ [54].

IV. HYPER-NETWORK MODEL OF SAS

A. MODEL

The T1-1 transmission substation model in IEC 61850 has one incoming line and two outgoing lines. Although it has a simple structure, its protection scheme and associated control functions are in commonly used for other types of transmission substations. Fewer lines and equipment make it easy to extend this model to the logical nodes tier and to be depicted in a limited figure area. Therefore, a T1-1 small-size transmission substation is used as an example in this study. The functions of a T1-1 SAS are shown in the left part of Fig. 1. Each function consists of multiple logical nodes (LNs). A logical node (LN) is a subfunction located in a physical node, which exchanges data with other separate logical entities. The links between logical nodes are listed in TABLE 2. The T1-1 substation has four bays: E01, E02, E03 and D01. The E01 and E03 are identical in structure and function. Using the distance protection in E03 as an example, the green rectangles in the red circle F6 are the logical nodes which participate in this function. In the right part of Fig. 1, green rectangles represent logical nodes, blue ellipses represent the three levels that are listed in TABLE. 3, and red circles represent functions F5 and F6. F5 is a metering and measurement function that contains several LNs such as MMXU, MMTR, TVTR, TCTR and IHMI. Measuring (represented as MMXU) is for the purpose of operation. It acquires data from current transformers and voltage transformers, and calculates the measurands. For example, r.m.s. values for current and voltage can be calculated in F5. These values are normally used for operational purposes such as power flow supervision and management, screen displays, and state estimation. Metering (represented as MMTR) is for the purpose of commercial behaviors. It acquires data from current transformers and voltage transformers and calculates the energy. F6 is the distance protection function containing several LNs such as

TABLE 2. Logical node connection relationships of each function.

Function attribute	Logical node connection relationships
F1	(TVTR, MMXU), (TVTR, MMTR), (TCTR, MMXU), (TCTR, MMTR) , (MMTR, IARC),(MMXU, IHMI), (IARC, IHMI)
F2	(TVTR, PDIS), (TCTR, PDIS), (PDIS, XCBR), (PDIS, ITMI), (ITMI, ITCI), (PDIS, IHMI)
F3	(TVTR, PLDF), (TCTR, PLDF), (PLDF, XCBR), (PLDF, ITMI), (ITMI, ITCI), (PLDF, IHMI)
F4	(XCBR, CILO), (XSWI, CILO), (CSWI, XCBR), (CILO, CSWI), (ITCI, CSWI), (IHMI, CSWI)
F5	(TVTR, MMXU), (TVTR, MMTR), (TCTR, MMXU), (TCTR, MMTR), (MMTR, IARC), (MMXU, IHMI), (IARC, IHMI)
F6	(TVTR, PDIS), (TCTR, PDIS), (PDIS, XCBR), (PDIS, ITMI), (ITMI, ITCI), (PDIS, IHMI)
F7	(TVTR, PLDF), (TCTR, PLDF), (PLDF, XCBR), (PLDF, ITMI), (ITMI, ITCI), (PLDF, IHMI)
F8	(XCBR, CILO), (XSWI, CILO), (CSWI, XCBR), (CILO, CSWI), (ITCI, CSWI), (IHMI, CSWI)
F9	(TVTR, PDIS), (TCTR, PDIS), (PDIS, XCBR), (PDIS, ITMI), (ITMI, ITCI), (PDIS, IHMI)
F10	(TVTR, MMXU), (TCTR, MMXU), (MMXU, ATCC), (ATCC, IHMI), (ATCC, YLTC)
F11	(TVTR, PTDF), (TCTR, PTDF), (XCBR, PTDF), (PTDF, ITMI), (ITMI, ITCI), (PTDF, IHMI)
F12	(TVTR, PTOV), (TCTR, PIOC), (PIOC, ATCC), (PTOV, ATCC), (ATCC, IHMI), (ATCC, YLTC)

IHMI, ITCI, ITMI, PDIS, TCTR, TVTR and XCBR. The line distance protection starts and trips in cases when the changes in line impedance, admittance or reactance exceed the predefined limits [55]. The blue solid line between the logical nodes represents logical connections, which is the communication link between logical nodes. It is defined as an edge in a network model. According to [56], only data contained in logical nodes can be exchanged. The purple dashed line represents the mapping of the logical node to the device.

In a normal network model, the connections between logical nodes are obvious, but the logical node's participation in different functions is difficult to show. A hyper-network model can clearly show this participation. In the hyper-network model of SAS, a function which consists of a set of logical nodes is considered a hyper-edge. In this way, the logical node that participates in multiple functions is obvious. The incidence matrices and adjacency matrices in the network model and in the hyper-network model can be derived from TABLE 1. These matrices are used to calculate the centrality measures to identify the critical elements in an SAS.

At the station level, the CALH signals an alarm and warns the operator to take action. A RBRF is a breaker failure protection that is a back-up protection and is activated only when the main protection fails. Man-in-the-loop and back-up protection are not considered in this paper. Therefore, CALH and RBRF are not included in TABLES 2 and 3.

TABLE 3. Levels of SAS.

Level name	Logical nodes	Full name
Station level	IHMI	Human Machine Interface
	ITCI	Telecontrol Interface
	ITMI	Telemonitoring Interface
	IARC	Archiving
Bay/unit level	PLDF	Differential line protection
	ATCC	Automatic Tap Changer Control
	CSWI	Switch Controller
	CILO	Interlocking Bay/Station
	PTDF	Differential transformer protection
	PTOV	(Time) Overvoltage protection
	PIOC	Instantaneous overcurrent or rate of rise protection
	MMXU	Measurand Unit /Op.
	PDIS	Distance protection
	MMTR	Metering/Acquisition And Calculation)
Process level	XCBR	Circuit Breaker
	XSWI	Disconnector
	TVTR	Voltage Transformer
	YLTC	Tap Changer
	TCTR	Current Transformer

B. TOPOLOGY ANALYSIS

General graphs cannot fully characterize some real world networks. While analyzing the T1-1 substation, the logical node must be attributed to the functions it participates in. This can be performed with a hyper-network model described above or a bipartite graph model in which logical nodes and functions are divided into two categories. However, only the connections between the two categories in a bipartite graph are shown. With a bipartite graph, analyzing connectivity, aggregation and other topological properties is difficult. It is mainly used to solve the maximum matching problem or perfect matching problem, which is not included in this study.

A hyper-graph, which can be described in terms of an analytic form has advantages. First, the matrix expression of hyper-graph can be easily processed with a computer. Second, the hyper-edge can be restructured in accordance with different requirements. This is an advantage for modeling reconfigurable systems. Finally, a matrix describes a snapshot of a fixed structure and a series of snapshots correspond to a series of moments. This makes it possible for a hyper-graph to simulate a time-varying system. However, there are also drawbacks, such as the neglect of connections between nodes. Moreover, some indices are difficult to comprehend intuitively or to extend from a general graph. Therefore, we choose typical indexes from general graph and we extend them to hyper-graph for a detailed analysis.

The heterogeneous logical nodes in an SAS network play different roles in structure and function. Identifying critical nodes is important because it helps with properly establishing the defense strategies of the SAS. Researchers in computer science and physics have studied critical node identification methods. Algorithms have been proposed and their criteria for identifying critical nodes are diverse. There does not exist a universal index suitable for every situation.

A comprehensive understanding of the similarities and dissimilarities in different methods can help us make the correct selection in application.

The network topological structure determines the influence of every node in it. The majority of existing critical node identification methods only use the structural information without considering the specific dynamic process. Structural centrality measures are proposed to evaluate the nodes' importance in terms of the structural information [57]. The influence of a node can be determined by its ability to impact others. Two categories of centrality measures, neighborhood-based centralities and path-based centralities, are summarized in [57]. A straightforward measure called degree centrality is a typical neighborhood-based centrality, which is defined by counting the number of a node's immediate neighbors. According to degree centrality, the more neighbors a node has, the more critical it is. While considering the information propagation process, a node is more critical when the paths through it spread information faster and broader. These can be calculated by path-based centralities.

Identifying critical elements in the general logical function model of SAS according to IEC 61850 series is the research objective in this study. As mentioned above, it can be represented as an undirected and unweighted graph or a hyper-graph. LNs are nodes, the logical link between a pair of LNs is an edge, and a function is a hyper-edge. The simple parameters of the T1-1 network are listed in Table 4. The T1-1 network is small because its number of nodes is 19. Its average degree centrality is far less than the number of nodes; thus, this network is sparse, like some technical networks.

TABLE 4. The simple parameters of T1-1's network.

Name	Number
Number of nodes	19
Connected components	1
İsolated nodes	0
Network diameter	5
Network radius	3
Clustering coefficient	0.048
Network centralization	0.199
Network density	0.211
Network heterogeneity	0.458
Characteristic path length	2.322
Avg. Number of neighbors	3.786

In this graph model, structural centralities help us to determine the LNs that are more critical. First, neighborhood-based centralities are discussed. Degree centrality is the simplest measure to evaluate a node's influence, which can be calculated by the number of its neighbors and is equal to the number of its connections. This measure is widely used because of its simplicity and good performance in some scenarios. For instance, attacks on nodes with a larger degree destroy the scale-free networks and exponential network more effectively than attack on nodes with other complicated indexes such as betweenness centrality, closeness centrality and eigenvector centrality [58]. A frequency distribution histogram of the T1-1 network is similar to the Poisson distribution. It can resemble an exponential network where degree centrality can then be selected to analyze the importance of the nodes under data attack. In addition, LocalRank is a centrality measure which fully considers all the fourth-order neighbors of each node. It is not suitable for the T1-1 network because its characteristic path length is less than 3. ClusterRank considers both the nearest neighbors and the interactions among them [57]. However, it is defined in a directed network, rendering it unsuitable for the T1-1 network. Since the network diameter and radius are 5 and 3 respectively, the coreness values of all nodes are very small and indistinguishable. Therefore, a coreness measure is unsuitable as well.

Among path-based centralities, the eccentricity of a node is the maximum distance of all the shortest paths to the other nodes. Maximum indexes fail to evaluate the importance of nodes because it is affected by unusually long paths in a network model. Closeness centrality can be calculated by the inverse of the harmonic mean distances, rendering it easily affected by the extreme values, particularly the shortest path lengths. Unlike closeness centrality, Katz centrality is more comprehensive because it considers all the paths [57], which increases its computational complexity. The subgraph centrality of a node is defined as a weighted sum of the numbers of all closed paths starting from and ending at it. Compared with the betweenness centrality of a node, which can be computed by counting all of the shortest paths passing through it, the subgraph centrality of a node is more suitable for this study because data attack on a closed loop information flows can easily confuse the LN.

In this study, degree centrality, which is a neighbor-based centrality, and subgraph centrality, which is a path-based centrality, are selected as the main indexes to identify the critical LNs in the T1-1 network model from a topological structure aspect. Additionally, they are able to be extended to hyper-graph easily and clearly defined in Section III. In Part C of Section IV, the comparative analysis of these centralities between a network model and hyper-network model is discussed.

C. CENTRALITY ANALYSIS

We use the concepts of degree centrality and sub-graph centrality, which have been extended to hypergraphs in [55]. These concepts describe the different node characteristics that enable the nodes to be ranked in the order of importance in the hyper-network. The first parameter indicates the participation of the node in different hyper-edges, and the second parameter characterizes the participation of the node in different sub-hypergraphs. In Fig. 2 the colored circles are logical nodes in T1-1, where the size of each circle represents a node's degree centrality and the color of each circle indicates its sub-graph centrality. The degree centralities of logical nodes in a network model and hyper-network model can be calculated by their corresponding incidence matrices and adjacent matrices.

In the hyper-network model, a logical node's degree centrality and sub-hypergraph centrality can be calculated

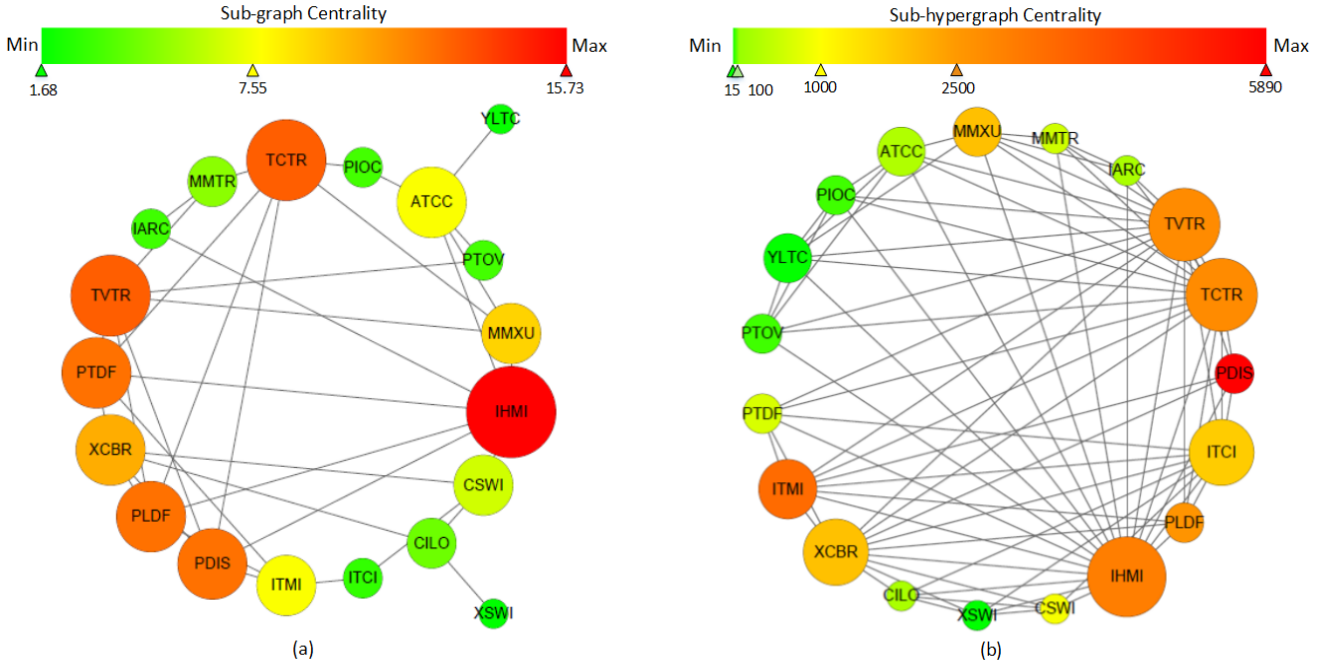

FIGURE 2. (a) network model of T1-1. (b) hyper-network model of T1-1.

by (10) and (11) respectively. In the network model, the degree centrality and subgraph centrality can also be calculated using (8) and (9), however, the incidence matrix $I(H)$ and adjacent matrix $A(H)$ should be replaced by the corresponding definitions of $I(G)$ and $A(G)$ in normal graph theory. The entry b_{ij}^G of $I(G)$ is defined in (12) and the entry a_{ij}^G of $A(G)$ is defined in (13).

$$b_{ij}^G = \begin{cases} 1, & v_i \in e_j^G \\ 0, & v_i \notin e_j^G \end{cases} \tag{12}$$

$$a_{ij}^G = \begin{cases} 1, & \text{if } (v_i, v_j) \in E^G \\ 0, & \text{if } (v_i, v_j) \notin E^G \end{cases} \tag{13}$$

where e_j^G is an edge and E^G is the set of edges in graph theory.

Significant differences can be observed when comparing the rankings introduced both by different centrality measures and in different network models. First, we analyze the degree centrality. The degree centralities of logical nodes in the network model and hyper-network model can be calculated by the corresponding incidence matrices. The relative degree centralities in these models are plotted in Fig. 3.

The top three most central nodes in the two models are identical. They are IHMI that represents human-machine interface action and data, TCTR that represents a current transformer's device and data, and TVTR that represents a voltage transformer's device and data. These three logical nodes are the most central ones and have more connections with other nodes; they appear most frequently in more functions represented as hyper-edges. These three logical nodes are the most vulnerable nodes based on the degree of centrality, and disabling one of them will exert a tremendous influence on the SAS.

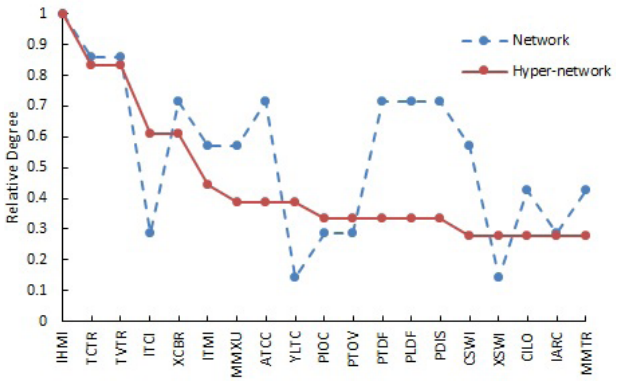

FIGURE 3. Ranking of logical nodes according to the relative degree.

The ranking of the other nodes in the hyper-network is different from the ranking in the network. For instance, ITCI is ranked as the fourth logical node in the hyper-network but does not appear among the top ten logical nodes in the network. This implies that although ITCI has fewer connections with other logical nodes, it appears in more hyper-edges that represent more different functions in the hyper-network. ITCI participates in 8 functions and has 2 connections with other logical nodes, whereas PDIS participates in only 3 functions even though it is ranked in the top three and has 5 connections with other logical nodes in the network model. The network model does not provide the number of functions in which a particular logical node participates. However, this

information can be obtained directly from the hyper-network model. The degree in the hyper-network model corresponds to the number of functions in which a logical node participates. The node with a greater degree in the hyper-network plays an important role in the system operation because disabling such logical node through data jamming has a larger impact on the system and the deviation produced by data tampering with such logical node is spread to more functions.

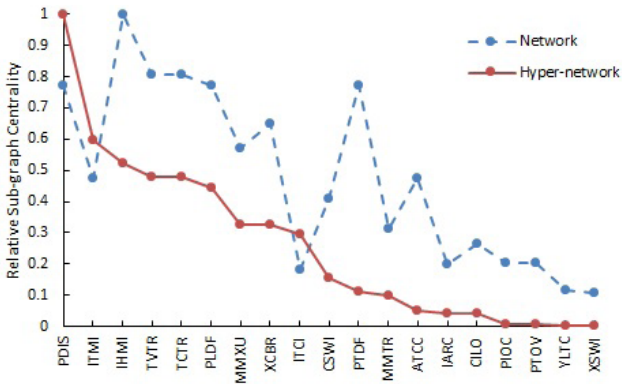

FIGURE 4. Ranking of logical nodes according to the relative sub-graph centrality.

The second measure discussed here is the sub-graph centrality. As shown in Fig. 4, there are significant differences in the ranking of the nodes' relative sub-hypergraph centrality compared with the relative sub-graph centrality calculated in the network model. PDIS is ranked as the most central node according to sub-hypergraph centrality, followed by ITMI and IHMI. ITMI is the second central node in the hyper-network model but is not among the top five logical nodes in the network model, whereas PTDF exhibits the opposite trend.

PDIS, for example, has the maximum sub-hypergraph centrality, which implies that there are more closed walks of different lengths starting and ending at PDIS than at other logical nodes. The contribution of these closed walks decreases as the length of the walks increases in the derivation of (11) [54]. Therefore, PDIS's closed walks pass through more functions, and the influence of data attack aiming at PDIS will spread more quickly because PDIS has many shorter closed walks.

The functions, logical nodes and logical connections in Bay E03 are given in Fig. 5(a), similarly for Bay E01. Fig. 5(b) shows the functions, logical nodes and logical connections in Bay E02 and D01. The greater the sub-hypergraph centrality of a logical node, the faster the influence of data attack aiming at it accumulates and spreads. The greater the degree centrality of a logical node in the hyper-network, the wider the range of direct influence it has after a data attack.

The degree and sub-graph centrality in a network model can only reflect the relationship between logical nodes. However, in the hyper-network model they express more functional information through a hyper-edge, which represents a set of logical nodes in the same function in this study.

V. EFFECTIVENESS ANALYSIS

A. A CYBER-PHYSICAL SYSTEM MODEL

The hyper-network model of SAS is applied to build a CPS model. The physical system is the IEEE 14 Bus test power system. In a power system layout, a bus usually represents a substation. If a transformer is present between two buses, the assumption that the transformer and its associated buses are located in the same substation is reasonable. Therefore, the cyber system consists of 10 nodes and there are 11 nodes if the control center is included. The cyber topology is shown as the blue circles and lines in Fig. 6. In each substation S/S k, the SAS consists of operating, protecting and monitoring functions. A function consists of subparts called logical nodes, which only exchange data with each other. In Fig. 6, the layered chart in the left side represents the interlocking function in Bay E01. It consists of six logical nodes: IHMI, ITCI CILO, CSWI, XCBR, and XSWI, which are defined in the IEC 61850 series.

B. EVALUATION METHODS OF EFFICIENCY AND DAMAGE

A logical node that is suffering from data jamming can not work effectively. When it is not working, the node and its associated logical connections are deleted from the network model and hyper-network model. If a logical node is suffering from data tampering, deviations will spread across the network via logical connections. The evolution of the SAS models under data attack can be observed in Fig. 5 and the IEC 61850 series. For example, when PDIS is under a data jamming attack, it cannot send data to XCBR in time. The circuit breaker rejects actions and the power line is not promptly disconnected. When PDIS is under a data tampering attack, it sends data to XCBR by error and the misoperation of the circuit breaker can occur.

The consequences of a data attack can be evaluated by the effectiveness indexes of SAS. There are two effectiveness indexes of SAS that are defined below according to attack scenarios. The first index is link efficiency $E_{Link}\ (S/S_k)$, which is used to assess the data link working efficiency of substation k's after a data jamming attack on its logical node n. It mainly considers the remaining logical connections between the two layers.

$$E_{Link}\ (S/S_k) = \frac{1}{N_{Level}-1}\left(\frac{\sum_{i\in G_S}\sum_{j\in G_B} e_{ij}^{n}}{\sum_{i\in G_S}\sum_{j\in G_B} e_{ij}^{initial}} + \frac{\sum_{i\in G_B}\sum_{j\in G_P} e_{ijij}^{n}}{\sum_{i\in G_B}\sum_{j\in G_P} e_{ij}^{initial}}\right) \tag{14}$$

where $e_{ij}^{initial}$ is an entry of the initial adjacency matrix in the network model and e_{ij}^{n} is an entry of the adjacency matrix in the network model after logical node n is attacked. G_S, G_B and G_P are the subscripts set of the logical nodes in the substation level, bay level and process level, respectively. The attributes of the levels of the logical nodes are listed in TABLE 3. N_{Level} is the number of levels.

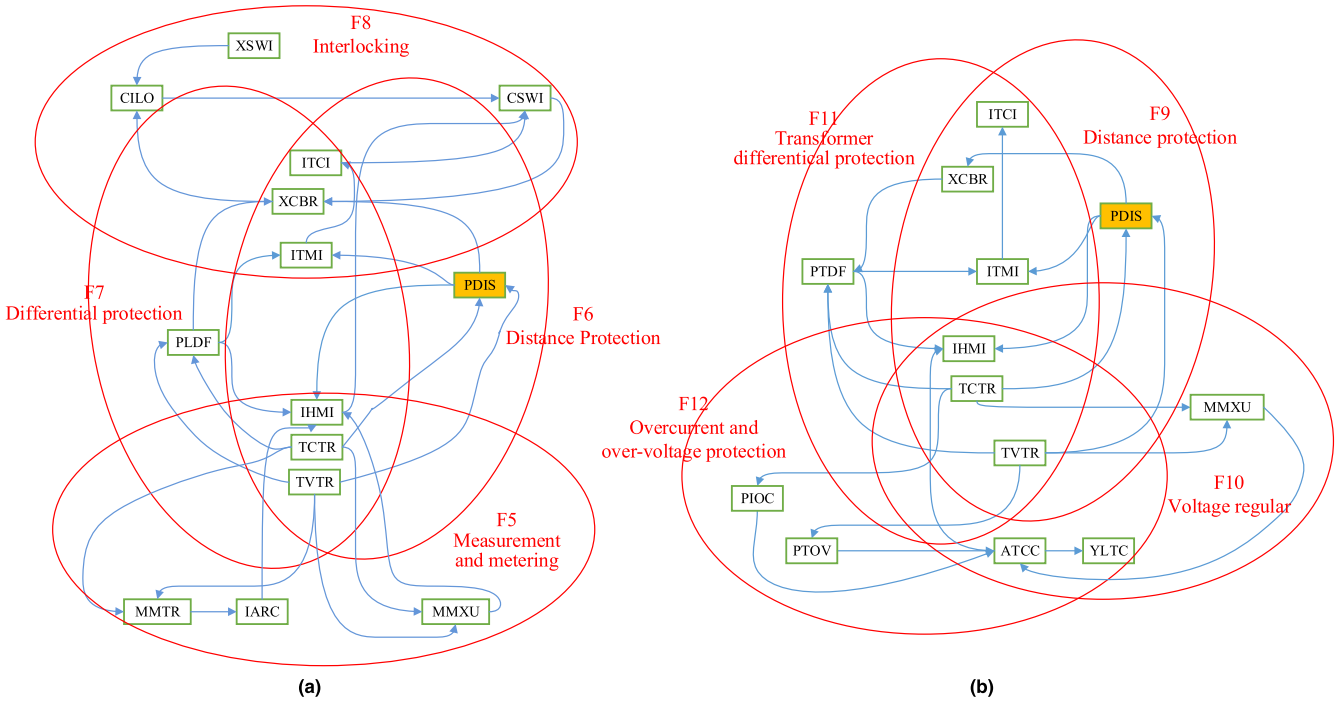

FIGURE 5. (a) Functions and logical nodes in Bay E03. (b) Functions and logical nodes in Bay E02 and Bay D01.

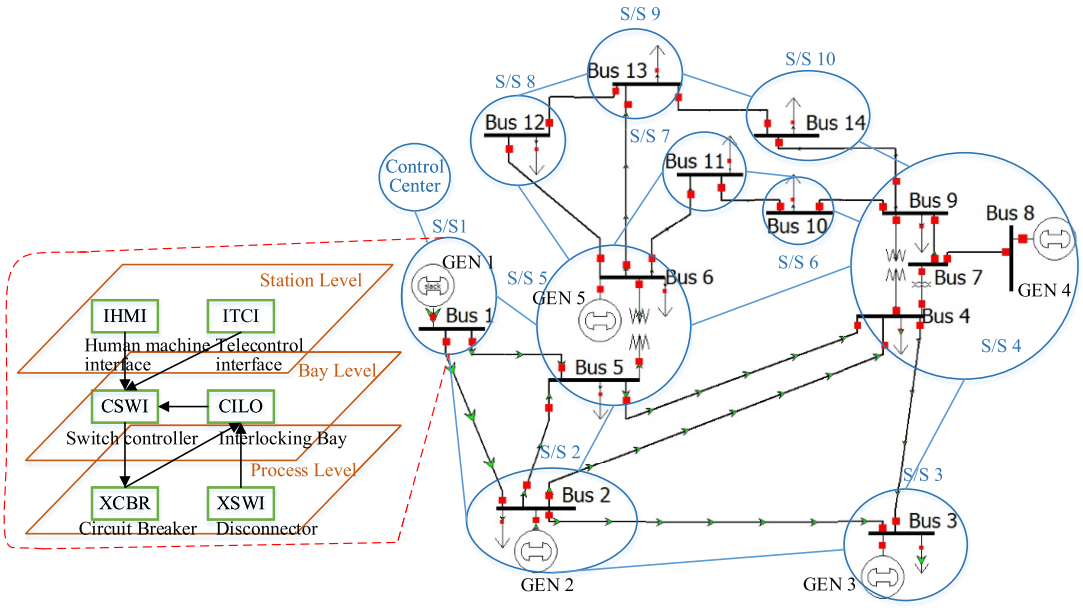

FIGURE 6. A Cyber-Physical System based on IEEE 14 Bus test power system.

The second index is function efficiency $E_{Function}(S/S_k)$, which can be used to assess the function realization efficiency of substation k after a data tampering attack on its logical node n. It is defined by the number of functions involved in the closed walks that start and end at logical node n.

$$E_{Function}(S/S_k) = \frac{Max\{C_{SH}(n)\}_{n\in[1,N_{LN}]} - C_{SH}(n)}{Max\{C_{SH}(n)\}_{n\in[1,N_{LN}]}} \quad (15)$$

where $C_{SH}(n)$ is the sub-hypergraph centrality of logical node n and N_{LN} is the number of logical nodes in substation k.

The integrated efficiency of the SAS of substation k can be defined in (16). It considers the connections between the logical nodes in the network model and the functional influence in the hyper-network model.

$$E(S/S_k) = \alpha E_{Link}(S/S_k) + (1-\alpha) E_{Function}(S/S_k) \quad (16)$$

Algorithm 1 Effectiveness Evaluation After Data Attack on Each LN in Some SASs

Input: IEEE 14 Bus test power system toppology and parameters. Each SAS's nodes, edges and hyper-edges.
Output: The nth LN's tag n, $E_n(CS)$, $E_n(PS)$ and $D_n(CPS)$ after data attack;
Initialize: The power system load and the kth SAS's incidence and adjacency matrices of the initial graphs and hyper-graphs $I\left(G^k_{Before}\right)$, $I\left(H^k_{Before}\right)$, $A\left(G^k_{Before}\right)$, $A\left(H^k_{Before}\right)$;
for $k \leftarrow 0$ to $N_{S/S}-1$ **do**
    Calculate initial efficiency of each substation $E(S/S_k)_{Before}$;
end for
Calculate initial power system load P_{Load_Before};
  for $n \leftarrow 0$ to $N_{LN}-1$ **do**
    for $k \leftarrow 0$ to $N_{S/S}-1$ **do**
      Do data link evolution after data attack on logical node n in S/S_k; /* Algorithm 2*/
      Calculate the effectiveness of substation $kE(S/S_k)_{After}$ after data attack;
    end for
  end for
  Calculate $E_n(CS)$, $E_n(PS)$and $D_n(CPS)$;
  Output n, $E_n(CS)$, $E_n(PS)$ and $D_n(CPS)$;

where $\alpha = 0.5$ is assumed here. If the number of substations in the cyber system is $N_{S/S}$, then the efficiency of the entire cyber system can be calculated by (17).

$$E(CS) = \prod_{k=1}^{N_{S/S}} \frac{E(S/S_k)_{After}}{E(S/S_k)_{Before}} \tag{17}$$

If there is only data jamming on the logical node n, it is deleted from the model. Deleting a logical node has no influence on functions sometimes, such as IARC. If there is only data tampering on the logical node n, it continues to work and its logical connections are not deleted from the model, and its data links also continue to work. This integrated efficiency index $E(CS)$ is applicable even when composite data attack mode appears in the cyber system. The composite attack mode is frequently used in current military electronic warfare.

Once the logical nodes in the process level, such as XCBR and XSWI, are affected by a data attack, the corresponding power line in the physical system is disconnected. The damage to the entire CPS should take load loss into consideration, which is defined as the normalized efficiency loss.

$$\begin{aligned} D(CPS) &= (1 - E(CS))(1 - E(PS)) \\ &= \left(1 - \prod_{k=1}^{N_{S/S}} \frac{E(S/S_k)_{After}}{E(S/S_k)_{Before}}\right)\left(\frac{P_{Load\_Before} - P_{Load\_After}}{P_{Load\_Before}}\right) \end{aligned} \tag{18}$$

where $E(PS) = P_{Load\_After}/P_{Load\_Before}$ is the load supply efficiency of the power system.

Algorithm 2 Data Link Evolution After Data Attack on Logical Node n in S/S_k

Input: Data attack target LN n and logical nodes in process level set Λ;
Output: The kth substation's tag k and the effectiveness $E(S/S_k)_{After}$ of substation k;
Initialize: The lth data link of logical node n in S/S_k has W_l walks;
if S/S_k is under attack **then**
for $l \leftarrow 0$ to $C^k_{Degree}(n) - 1$ **do**
    $t \leftarrow 0$;
    while $t <= W_l - 1$ **do**
if $LN_t \in \Lambda$ **then**
        Update matrices;
        Break;
      else
        $t \leftarrow t + 1$;
      end if
    end while
  end for
  Obtain matrices $I\left(G^k_{After}\right), I\left(H^k_{After}\right), A\left(G^k_{After}\right)$ and $A\left(H^k_{After}\right)$;
  Calculate $E(S/S_k)_{After}$;
else
  After $\leftarrow$ Before;
end if
Output k and $E(S/S_k)_{After}$;

Effectiveness of the CPS after a data attack on each logical node type in some SASs is evaluated as the pseudo-code of Algorithm 1 presented below. A core step in Algorithm 1 is shown in Algorithm 2.

C. RESULTS AND ANALYSIS

We analyze the effectiveness of the CPS after data attacks on each individual logical node of substation S/S1 shown in Fig. 6. Taking PDIS as an example, the data jamming attack on PDIS can force its next logical node XCBR to refuse operation for the distance protection function. This refusal of operation for XCBR can cause a line overload. Then the line may fail to work. A data tampering attack on PDIS can make its next logical node XCBR misoperate with the distance protection function. This misoperation of XCBR can make the line quit. TABLE 4 shows that when PDIS is attacked, the integrated efficiency of S/S1 is the lowest. The analysis of the physical system indicates that when PDISs in S/S1 are attacked, the influence can arrive at XCBRs in a walk, causing the three lines to quit and the generator GEN 1 to be cut. The attacks on PDISs have the greatest impact on the S/S1 in the shortest time. IHMI is allocated at the station level, taking part in every function of the SAS because it has hyper-degree of 12. However, the walks of its messages to the logical nodes in the process level is greater than those of PDIS. The IEEE 14 Bus test power system is designed to

TABLE 5. The efficiencies when each logical node in S/S_1 is attacked.

n	LN	Full name	E_{Link} (S/S_1)	$E_{Function}$ (S/S_1)	$E(S/S_1)$
0	PIOC	Instantaneous overcurrent or rate of rise protection	0.974	0.992	0.983
1	PTOV	(Time) Overvoltage protection	0.974	0.992	0.983
2	PTDF	Differential transformer protection	0.830	0.889	0.859
3	YLTC	Tap Changer	0.974	0.997	0.985
4	ATCC	Automatic Tap Changer Control	0.928	0.948	0.938
5	CSWI	Switch Controller	0.883	0.842	0.863
6	XSWI	Disconnector	0.974	0.997	0.986
7	CILO	Interlocking Bay/Station	0.947	0.958	0.953
8	PLDF	Differential line protection	0.830	0.555	0.693
9	ITCI	Telecontrol Interface	0.955	0.703	0.829
10	ITMI	Telemonitoring Interface	0.864	0.402	0.633
11	XCBR	Circuit Breaker	0.868	0.674	0.771
12	PDIS	Distance protection	0.830	0.000	0.415
13	IHMI	Human Machine Interface	0.727	0.475	0.601
14	IARC	Archiving	0.955	0.958	0.956
15	TCTR	Current Transformer	0.842	0.521	0.682
16	MMTR	Metering/Acquisition And Calculation)	0.902	0.902	0.902
17	MMXU	Measurand Unit /Op.	0.902	0.673	0.788
18	TVTR	Voltage Transformer	0.842	0.521	0.682

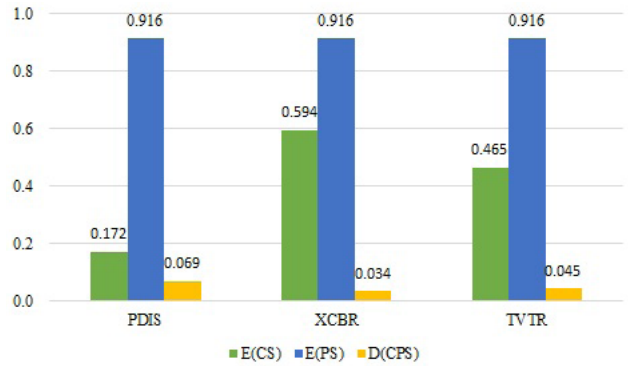

FIGURE 7. The effectiveness indexes after data attack on a logical node in S/S1 and S/S2.

have a large redundant capacity. Therefore, if the three lines in S/S1 quit, it will not affect the power system's load supply efficiency $E\,(PS) = 1$, and the damage to the CPS remains zero with $D\,(CPS) = 0$.

In TABLE 5, there are differences when the logical nodes are sorted in descending order of $E_{Link}\,(S/S_k)$ and $E\,(S/S_k)$. This is because the $E_{Link}\,(S/S_k)$ column only considers the connections between logical nodes, and the $E\,(S/S_k)$ column considers the f unctional influence on the hyper-network model.

If we want $E\,(PS) \neq 1$, which implies that there is load loss in the power system, we must design the composite data attack strategies to target e ach type of logical nodes in the multiple substations or the control center. For example, when the PDISs in substation S/S1 and S/S2 are under data attack, there will be 21.7MW load loss in the power system and the damage of the CPS is 6.9% as shown in Fig. 7.

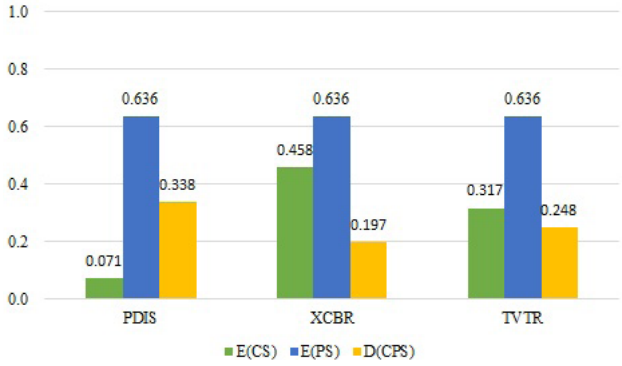

FIGURE 8. The effectiveness indexes after data attack on a logical node in S/S1, S/S2 and S/S3.

When the PDISs in substation S/S1, S/S2 and S/S3 are under data attack, there will be 94.2MW load loss in the power system and the damage of the CPS is 33.8% as shown in Fig. 8. In future studies we will consider protection measures such as firewalls and gateways, and the evaluation process will be an offence and defense game.

VI. CONCLUSION

This paper introduces the concept of a hyper-network to model a CPS according to IEC 61850. Considering the complexity of the cyber and physical interaction, extended centrality measurements in hypergraph are used to identify the critical elements in CPS. An effectiveness evaluation method of CPS after data attack is proposed in this work. This method considers not only the influence on connections between logical nodes, but also the functional influence and load loss after data attack. This work is helpful for guiding the white box experiments of defense technology against data attacks. This paper only analyzes the impact of attacks on one logical node type (in a station or in several stations). More complex composite data attack strategies targeting multiple logical node types will be studied in the future. The game model in which a successful attack action is considered as a probabilistic event related to offense and defense measures can also be established in future research.

REFERENCES

[1] R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th Design Autom. Conf.*, Jun. 2010, pp. 731–736.
[2] Y. Mo *et al.*, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[3] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
[4] S. Xin, Q. Guo, H. Sun, B. Zhang, J. Wang, and C. Chen, "Cyber-physical modeling and cyber-contingency assessment of hierarchical control systems," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2375–2385, Sep. 2015.
[5] J. Wei, D. Kundur, T. Zourntos, and K. L. Butler-Purry, "A flocking-based paradigm for hierarchical cyber-physical smart grid modeling and control," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2687–2700, Nov. 2014.
[6] J. Hu, J. Yu, J. Cao, M. Ni, and W. Yu, "Topological interactive analysis of power system and its communication module: A complex network approach," *Physica A, Stat. Mech. Appl.*, vol. 416, pp. 99–111, Dec. 2014.

[7] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, Feb. 2011.

[8] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Jul. 2016.

[9] Y. Xiang, L. Wang, and Y. Zhang, "Power grid adequacy evaluation involving substation cybersecurity issues," in *Proc. IEEE Innov. Smart Grid Technol. Conf.*, Feb. 2015, pp. 1–5.

[10] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[11] X. Liu, M. Shahidehpour, Z. Li, X. Liu, Y. Cao, and Z. Li, "Power system risk assessment in cyber attacks considering the role of protection systems," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 572–580, Mar. 2017.

[12] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2015.

[13] A. Ashok, S. Krishnaswamy, and M. Govindarasu, "PowerCyber: A remotely accessible testbed for cyber physical security of the smart grid," *Proc. IEEE Innov. Smart Grid Technol. Conf.*, Sep. 2016, pp. 1–5.

[14] A. Ashok, P. Wang, M. Brown, and M. Govindarasu, "Experimental evaluation of cyber attacks on automatic generation control using a CPS security testbed," in *Proc. IEEE Power, Energy Soc. General Meeting*, Jul. 2015, pp. 1–5.

[15] A. Hahn and M. Govindarasu, "An evaluation of cybersecurity assessment tools on a SCADA environment," in *Proc. IEEE Power Energy Soc. General Meeting*, Jul. 2011, pp. 1–6.

[16] V. K. Singh, A. Ozen, and M. Govindarasu, "Stealthy cyber attacks and impact analysis on wide-area protection of smart grid," in *Proc. IEEE North Amer. Power Symp.*, Sep. 2016, pp. 1–6.

[17] Y. Chen, J. Hong, and C. C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Trans. Smart Grid*, to be published.

[18] S. K. Khaitan, J. D. Mccalley, and C. C. Liu, "Cyber-physical security testbed for substations in a power grid," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Berlin, Germany: Springer, 2015, pp. 261–300.

[19] H. Lei, C. Singh, and A. Sprintson, "Reliability modeling and analysis of IEC 61850 based substation protection systems," *IEEE Trans. Smart Grid*, vol. 5, no. 5, pp. 2194–2202, Sep. 2014.

[20] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 235–244, Mar. 2013.

[21] M. X. Cheng, M. Crow, and Q. Ye, "A game theory approach to vulnerability analysis: Integrating power flows with topological analysis," *Int. J. Electr. Power Energy Syst.*, vol. 82, pp. 29–36, Nov. 2016.

[22] H. Qiu, Y. Zhicai, Q. Jichuan, and L. Zhipeng, "Topological structure modeling and analysis for cyber-physical systems," in *Proc. IEEE Inf. Technol. Artif. Intell. Conf.*, Dec. 2015, pp. 523–526.

[23] Y. Sheffi and C. F. Daganzo, "Hypernetworks and supply-demand equilibrium obtained with disaggregate demand models," *Transp. Res. Rec.*, vol. 673, pp. 113–121, Sep. 1978.

[24] A. Nagurney and F. Toyasaki, "Supply chain supernetworks and environmental criteria," *Transp. Res. D, Transp., Environ.*, vol. 8, no. 3, pp. 185–213, May 2003.

[25] A. Nagurney, "On the relationship between supply chain and transportation network equilibria: A supernetwork equivalence with computations," *Transp. Res. E, Logistics, Transp. Rev.*, vol. 42, no. 4, pp. 293–316, Jul. 2006.

[26] A. Nagurney, J. Cruz, and D. Matsypura, "Dynamics of global supply chain supernetworks," *Math. Comput. Model.*, vol. 37, nos. 9–10, pp. 963–983, May 2003.

[27] A. Nagurney and J. Dong, "Management of knowledge intensive systems as supernetworks: Modeling, analysis computations, and applications," *Math. Comput. Model. Int. J.*, vol. 42, nos. 3–4, pp. 397–417, Aug. 2005.

[28] A. Nagurney and J. Dong, "Multidriteria decision-making in financial networks," in *Supernetworks: Decision-Making for the Information Age*. Cheltenham, U.K.: Edward Elgar, 2002, pp. 22–35.

[29] S. Grünewald, A. Spillner, S. Bastkowski, A. Bögershausen, and V. Moulton, "SuperQ: Computing supernetworks from quartets," *IEEE/ACM Trans. Comput. Biol. Bioinformatics*, vol. 10, no. 1, pp. 151–160, Jan. 2013.

[30] H. Zhang and C. Liu, "A method of entity relationship modeling of Internet of Things based on supernetwork," in *Proc. 6th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Sep. 2015, pp. 305–308.

[31] Z. Li and H. Wang, "Supernetwork model of knowledge management in paroxysmal public crisis," in *Proc. Int. Conf. Manage. e-Commerce e-Government (ICMECG)*, Sep. 2009, pp. 95–100.

[32] S. Fu-Li, L. Yong-Lin, and Z. Yi-Fan, "A military communication supernetwork structure model for netcentri c environment," in *Proc. Int. Conf. Comput. Inf. Sci. (ICCIS)*, Dec. 2010, pp. 33–36.

[33] F. Shi, C. Li, D. Qin, Y. Zhu, and F. Yang, "A complexity measure for military communication networks," in *Proc. Military Commun. Conf. (MILCOM)*, Nov. 2011, pp. 1708–1713.

[34] Z. Zou, F. Liu, S. Sun, L. Xia, and C. Fan, "Ripple-effect analysis for operational architecture of air defense systems with supernetwork modeling," *J. Syst. Eng. Electron.*, vol. 25, no. 2, pp. 249–264, Apr. 2014.

[35] Q. Zhao, S. Li, Y. Dou, X. Wang, and K. Yang, "An approach for weapon system-of-systems scheme generation based on a supernetwork granular analysis," *IEEE Syst. J.*, vol. 11, no. 4, pp. 1971–1982, Dec. 2015.

[36] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.

[37] K. Pan, A. M. H. Teixeira, M. Cvetkovic, and P. Palensky, "Combined data integrity and availability attacks on state estimation in cyber-physical power grids," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2016, pp. 271–277.

[38] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[39] Y. Hao, M. Wang, and J. H. Chow, "Likelihood analysis of cyber data attacks to power systems with Markov decision processes," *IEEE Trans. Smart Grid*, to be published.

[40] 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 Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016.

[41] W. Steve and J. Andress, "Tools and techniques," in *The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare in Theory and Practice*. Rockland, MA, USA: Syngress, 2012, pp. 51–66.

[42] M. McDowell. US-CERT. (2013). *Understanding Denial-of-Service Attacks*. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-015

[43] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *Trans. Inf. Syst. Secur. ACM*, vol. 14, no. 2, pp. 21–32, 2009.

[44] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 220–225.

[45] H. Sun, F. Gao, S. Kai, and B. Zhang, "Analog-digital power system state estimation based on information theory—Part I: Theory," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1640–1646, Sep. 2013.

[46] T. Yang, H. Sun, and A. Bose, "Transition to a two-level linear state estimator—Part I: Architecture," *IEEE Trans. Power Systems.*, vol. 26, no. 1, pp. 46–53, Feb. 2011.

[47] Q. Li, H. Sun, J. Wang, B. Zhang, W. Wu, and Q. Guo, "Substation three-phase nonlinear state estimation based on KCL," in *Proc. IEEE Power Syst. Conf. Expo.*, Mar. 2011, pp. 1–5.

[48] Q. Li, H. Sun, T. Sheng, B. Zhang, W. Wu, and Q. Guo, "Injection attack analysis of transformer false data in substation state estimation," *Autom. Electr. Power Syst.*, vol. 40, no. 17, pp. 79–86, Sep. 2016.

[49] A. L. Barabasi *et al.*, "Virtual round table on ten leading questions for network research," *Eur. Phys. J. B*, vol. 38, no. 2, pp. 143–145, Mar. 2004.

[50] C. Berge, "Hypergraphs and their duals," in *Graphs and Hypergraphs*. New York, NY, USA: Elsevier, 1973, pp. 389–391.

[51] Z.-T. Wang and Z.-P. Wang, "Elementary study of supernetworks," *Chin. J. Manage.*, vol. 5, no. 1, pp. 1–8, 2008.

[52] J. K. Kim and B. T. Zhang, "Evolving hypernetwroks for pattern classification," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Singapore, Sep. 2007, pp. 1856–1862.

[53] E. Estrada and J. A. Rodríguez-Velázquez, "Subgraph centrality in complex networks," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 71, no. 5, pp. 1–9, May 2005.

[54] E. Estrada and J. A. Rodríguez-Velázquez, "Subgraph centrality and clustering in complex hyper-networks," *Phys. A, Statist. Mech. Appl.*, vol. 364, no. 1, pp. 581–594, May 2006.

[55] *IEC Standard for Communication Network and Systems in Substations—Part 1: Introduction and Overview*, Document IEC 61850-1, 2003.

[56] *IEC Standard for Communication Network and Systems in Substations—Part 5: Communication Requirements for Functions and Device Models*, Document IEC 61850-5, 2003.
[57] L. Lü, D. Chen, X.-L. Ren, Q.-M. Zhang, Y.-C. Zhang, and T. Zhou, "Vital nodes identification in complex networks," *Phys. Rep.*, vol. 650, pp. 1–63, Sep. 2016.
[58] S. Iyer, T. Killingback, B. Sundaram, and Z. Wang, "Attack robustness and centrality of complex networks," *PLoS ONE*, vol. 8, no. 4, p. e59613, 2013.

YOUPING FAN was born in Jingzhou, Hubei Province, China, in 1970. He received the Ph.D. degree in control theory and control engineering from Chongqing University, Chongqing, China, in 2003.

He is currently a Professor with the School of Electrical Engineering, Wuhan University, Wuhan, China. His research interests are artificial intelligence and knowledge engineering, modeling and control of complex system, security analysis and risk control technology of power system, and parameter identification of power system.

JINGJIAO LI received the B.S. degree in electrical engineering and automation from Harbin Engineering University, Harbin, China, in 2007, and the M.S. degree in signal and information processing from the Yangzhou Marine Electronic Instrument Research Institute of CSIC, Yangzhou, China, in 2010. She is currently pursuing the Ph.D. degree in power system and automation with the School of Electrical Engineering, Wuhan University.

From 2010 to 2014, she was a Researcher and an Analyst with Beijing Tsingsoft Innovation Technology Co., Ltd., Beijing, China. Her research interest includes the performance evaluation of complex electronic information and attacking system, power system load forecasting and scheduling method, and modeling and analysis of CPS.

DAI ZHANG received the M.Eng. degree in electrical engineering from the University of Leicester, Leicester, U.K., in 2013. He is currently pursuing the Ph.D. degree with Wuhan University. His major research interests include power system planning and reliability evaluation, modeling, and analysis of CPS.