Optimizing Configuration of Cyber Network Considering Graph Theory Structure and Teaching-Learning-Based Optimization

(GT-TLBO)

M. Hamzeh, B. Vahidi, *Senior Member, IEEE* and A. F. Nematollahi

Abstract—**selecting the best configuration for a cyber-network system is considered as one of the major challenges in terms of reliability evolution of smart systems because of a specific relationship between power network system and cyber network. Although producing some possible cyber networks for one simple power system and selecting the best one does not need any formulas and can be done through trial and error as performed in previous studies, producing all possible n-th elements of cyber network that observe the cyber protocols and choosing the best one has not been done before. choosing the best configuration for any n-th elements cyber-network that can be connected to a bulk power network needs a robust and adequate computer algorithm considering cyber protocols and decision-making goals. In this paper, a novel method is proposed in order to introduce the best configuration for a cyber-network system to accommodate cyber protocols and have a remarkable effect on decreasing energy not supplied (EENS) compared with those previously studied. To this end, two mathematical concepts are proposed; graph theory to consider cyber protocols and teaching-learning-based optimization to select the best cyber configuration with minimum expected energy not supplied. During the first time, choosing the best configuration with each specific goal for *n*th devices of a cyber-network system is applicable by converting it into an $n \times n$ adjacency matrix and using the proposed graph theory mixed with teaching-learning-based optimization algorithm. Moreover, Monte Carlo simulation was used in this paper as one of the most precise probabilistic methods.**

The test results indicate that the proposed method selected for identifying the best configuration of a cyber-network system has significantly improved reliability indices compared to those in previous papers and it could be useful for every wide power-cyber network. Additionally, different types of cyber network are studied for validating the proposed method. This method is applied to the realistic feeder of Hormozgan Regional Electric Company as a smart pilot system.

Index Terms—**Cyber System, Power System, Cyber-Power Relation, Reliability, Graph Theory, TLBO, DG Units.**

I. Introduction

RECENTLY, the role of cyber security and communication system within the wide area of monitoring, protection, and control in large-scale power systems has become of utmost importance. Remarkable cyber-related revolution has also occurred by replacing traditional analogous communication system with digital and computer-based ones [1]. Moreover, the combinatorial extension of cyber and power network creating the new concept of cyber-physical system has been highlighted as another aspect of this revolution [2].

Due to wide extent of the communication system as well as increase in electrical energy consumption, researchers have become interested in assessing reliability of power and cyber networks simultaneously; consequently managing their interdependencies. In this regard, mal-operation of cyber networks not only affects these networks distractively but also brings about harmful effects on power network. So, adequacy evaluation of the whole system without considering cyber-power interdependencies is not a precise attempt [3-6].

In [7], the on-demand strategy was illustrated to show how cyber system should be configured to reach better performance for electrical network using error-dependent communication concept to explore dynamic network over communication systems.

Tullio Facchinettiet et al. [8] also proposed a novel method to use real-time scheduling techniques for controllable electrical load in cyber-physical power systems to get hold of an optimized upper band on power peak load.

The impact of three different cyber events on power grid was similarly analyzed in [9]. For this purpose, a real-time modeling of power system was used with three different cyber events. It should be noted that real-time digital simulator, synchro-phasor devices, as well as deter lab and network simulators were used for real-time modeling of end-to-end cyber-power systems in this paper.

Direct cyber-power interdependencies (DCPI) and indirect cyber-power interdependencies (IDCPI) had been already studied in [3-6]. Although the effect of cyber network on power network regarding reliability perspective has been considered but the influence of different configurations for cyber network on power system adequacy has not been investigated.

Authors are with Department of Electrical Engineering, Amirkabir University of Technology, Tehran 1591634311, Iran (Email: vahidi@aut.ac.ir).

In this regard, Falahati et al. [4] defined four types of cyber network configurations and evaluated expected energy not supplied (EENS) in a power system for each configuration. However, the optimal cyber configuration was not considered in this study.

Literature review could illustrate a significant consideration of cyber-power interdependences as well as the effect of cyber system and adequacy of the smart grid. Although in [3, 4], authors tried to identify the impact of a cyber-network system on a simple power system, these papers failed to present a comprehensive solution to identify the best configuration for the cyber network system within complicated networks and decision-making goals. Thus, this study proposed a novel method to select the best configuration for *n*th devices of a cyber-network system due to specific goals such as reliability evaluation. Accordingly, choosing the proper cyber system for a bulk and complicated power system was applicable by converting the cyber network into $n \times n$ adjacency matrix and using new numerical algorithms based on graph theory mixed with teaching-learning-based optimization algorithm (GT-TLBO). The proposed method was not only useful for decision-making concerning a complicated network for the first time but also illustrated that reliability indices had decreased for the simple network compared to those reported in previous papers. The rest of this paper is organized as follows. Section II introduces different cyber-power relations in a cyber-physical system. Section III discusses the stochastic reliability assessment of distributed generations and Monte Carlo simulation. In Sections IV and V, two laws of graph theory and their applications in cyber protocols are explained. Teaching-learning-based optimization in the proposed method is also delineated in Section VI. In Section VII, the importance of the proposed GT-TLBO algorithm is studied for each wide cyber network. Finally, the test results and conclusions are presented in Sections VIII and IX, respectively.

II. Cyber-power relation (CPR)

Cyber and power systems are internally connected to each other [3-6]. This means that abnormal operation of a cyber-network system can damage the normal performance of a power network. Failure in each element of cyber network can cause failure or inappropriate behavior of other elements of a power system also. In [4], authors have identified four types of relationship between cyber and power systems. It has been argued that if cyber element failure results in absolute failure of typical power element, the direct element-element relation (DEER) has occurred. Performance of a cyber-network system could also directly damage the operation of a special element in power system which is called direct network element relation (DNER). Furthermore, indirect element-element relation (IEER) could illustrate that failure in elements of a cyber-network system do not directly cause failure in power elements, but it could gradually affect the performance of power elements in its service life. If the failure in a cyber-network system has indirect and unfavorable effects on specification element of the power system, it is identified as indirect network element relation (INER). For example, failure in one Energy Management Unit (EMU) in cyber network might cause failure in the specific circuit breaker that had peer-to-peer connection with it. Besides, this is a direct element-element relation (DEER) failure. The reason for occurrence of this phenomenon is that incorrect data from related circuit breaker has reached the server when EMU had failed. In this respect, it was supposed by the server that circuit breaker had failed and a command of disconnecting circuit breaker has been issued. Within a direct network element relation (DNER), mal-operation could occur in the entire cyber elements if the server of a cyber-network system had failed in a way that the elements which were interdependent would operate inappropriately. Although malfunction of monitoring devices could not lead to failures in typical elements of the power system, it could cause incorrect decision-making by the operator that would jeopardize performance of some power elements. This was a good example for indirect element-element relation (IEER). When backing up relay protection supporting the main relay protection did not operate in the arranged coordination time, the out-service period of power element could increase and an indirect network element relation (INER) could occur.

III. Graph theory in CYBER NETWOK

The mathematical structure identifying relations between all objects of one graph including nodes and edges is called graph theory [10]. The given theory is employed in lots of sciences such as biology, physics and etc. for system modeling. In this respect, an electrical network can be modeled as a graph where electrical devices and electrical connections are considered as its vertices and edges, respectively.

The cyber network can be assumed as a graph because cyber devices such as energy management units (EMU), switches, and servers are considered as vertices and communication connections are known as edges. In order to observe the rules and protocols within the standard cyber- network system, graph theory rules should be applied.

Although it is possible to use trial and error for selecting the best cyber configuration as in [4] within a simple cyber-power network, it is necessary to use a robust and reliable algorithm that chooses the best cyber network system for a specified goal considering all different protocols of cyber network in vast and complicated networks having a lot of devices and connections.

A. *Kosaraju's depth first search-based (DFS) algorithm in graph theory*

One of the major concepts of graph theory is connectivity [11]. Accordingly, a graph is connected when at least one route exists between vertices of the network. To understand whether the graph is connected or not, Kosaraju DFS-based algorithm is used.

In the cyber network, all devices of network should be connected to each other, and no part should be islanded. For this purpose, Kosaraju's DFS-based algorithm of graph theory can be used. This algorithm confirms that all devices of a cyber-network system such as servers, EMUs, and switches as nodes should be strongly connected to each other via communication connectors as edges. The following algorithm shows steps of this algorithm clearly [12]

```
Algorithm 1: Dijkstra algorithm
Take initial matrix from TLBO
Choose one of the vertex randomly
Mark this vertex
Count the marked vertex
1) The unmarked neighbors of marked vertex should be marked and counted
If all neighbors of each marked vertex have been marked
If the number of marked vertices= the number of total vertices
Send Kosaraju is true
Else
Send Kosaraju is false
End
Else
Go to 1
End
```

In the first step, the adjacency matrix is taken from TLBO algorithm. Then one of the vertices is chosen, marked and counted in that matrix. The neighbors (vertices that directly connected to the marked vertex) are marked and counted too. This process is repeated until all neighbors of the marked vertices are chosen. If the number of counted vertices is equal to the total number of vertices, it means that all vertices of the matrix are connected to each other; consequently connectivity that is one of the important protocols of the cyber network is true. The example in the later section will show these processes.

B. Dijkstra algorithm in graph theory

Dijkstra algorithm can be used to find the shortest path between nodes in either directed or undirected connectivity graphs [13]. In addition, this algorithm specifies if there is a path between typical pair vertices or not. Likewise, it generates the shortest path tree (SPT) which contains source vertex and sink one.

Within the cyber-network system, each EMU should be connected to at least one server by at least one route. To this end, servers must control and manage the cyber network, and it is necessary to be connected to each energy management unit for complete connection to a power network. Accordingly, Dijkstra law confirms at least one path exists between each EMU and at least one server. The steps of this algorithm are given below clearly:

```
 Algorithm 2: Dijkstra algorithm
Take initial matrix from TLBO
For i=1 to $N_{EMU}$
 $A_i$ is origin
For j=1 to Nsr
 $B_j$ is destination
While $B_j$ is marked
 Mark $A_i$ vertex
 1) Mark neighbors of the marked vertex
 If all neighbors of each marked vertx have been marked
 If Bj is not marked
 Send $A_i$ is false
Send Dijkstra is false
Quite the while
End
End
If $B_j$ is marked
Send $A_i$ is tru
Quite the for % there is the path between i-th EMU and at least one server
Else
Go to 1
End
End
End
If all of Ai are tru
Send Dijkstra tru
End
```

Where N_{EMU}, N_{sr}, A_i and B_j are the number of EMU vertices, the number of server vertices, i-th vertex of EMU vertices and j-th vertex of server vertices, respectively. In this algorithm, A_i is the origin and B_j is the destination. The algorithm tries to specify if there any paths between each origin and destination or not. In the first step, the matrix is taken from the last part. A_i and B_j are chosen randomly. Ai should be marked and neighbors of Ai should be marked too. These processes are repeated for the neighbors of marked vertices. If the algorithm can reach the Bj and destination is marked, the Dijkstra is true for Ai. If all origins can reach to at least one destination, the Dijkstra is true for cyber network. An example in the later section will show these processes.

In fact, the first law and the second law of graph theory are the congestions of optimization algorithm for checking the protocols of cyber network for the zero-one matrix that is produced by TLBO optimization.

IV. TEACHING LEARNING BASED OPTIMIZATION (TLBO)

Recently, development of computer hardware and software has lowered the time and cost of solving complex problems. However, knowledge of skillful people is required to solve such problems. Since each expert has suggested a different method, a variety of solutions may be obtained. This makes the achieved solutions unreliable and inaccurate as the desired ones. Numerous attempts have been made for preparing a method which can optimally solve a problem without any previous knowledge of computers while the achieved solution would be trustworthy and low-cost. To meet this goal, researchers turned to meta-heuristic algorithms. In these types of algorithms, problems can be designed optimally using general knowledge.

R.Rao et al. presented a new meta-heuristic method as a population-based algorithm like other optimization methods [14,15]. This method simulates the teaching-learning process between a teacher and students in a classroom. Unlike other traditional optimization algorithms, the teaching-learning-based optimization (TLBO) algorithm is independent of optimization parameters. For example, the parameters of PSO and GA depend on weights (W1, W2) and the maximum value of velocity, crossover and mutation probability, as well as selection methods; respectively. This optimization algorithm has three main steps which are explained as follows:

A. *Initialization*

Like other evolutionary optimization algorithms, TLBO generates an initial population in which each member is considered as a student. N_{std} is the total number of students and N is considered as the problem dimension. Each student's score is defined as the following vector:

$$L_j = \left[X_j^1, X_j^2, X_j^3, \dots, X_j^N\right](j = 1,2,\dots,N_{std}) \qquad (1)$$

The objective function in this paper as EENS specifies each student's ability. According to the minimization nature of the problem, the student corresponding with minimum objective function is considered as a teacher of this population.

B. *Teacher phase*

The best solution for TLBO optimization is called teacher. The main responsibility of the teacher is to increase students' knowledge of teacher-student relationship. In order to increase the knowledge process, Eq.(2) is suggested. In this equation; L_T, Ls and L_{min} are teacher level, student level, and average students level in the classroom; respectively.

$$\begin{aligned} Ls^{new}{}_i &= Ls^{old}{}_i + r_i \left(L_T - T_f L_{\min}\right) \\ T_f &= Round\,(1+\mathrm{rand}[1,0]) \end{aligned} \qquad (2)$$

Where r_i is a random parameter in the range of [0- 1] and T_f stands for a random parameter in [1- 2] which is called teacher factor.T_f is not a fixed parameter and in each repetition. T_f could be either 1 or 2 and is determined randomly with equal probability. The random nature of T_f does not violate the independent optimization nature of parameters of the TLBO algorithm [14, 15].

C. *Student phase*

Within this step, students increase their knowledge by sharing information with each other. Two students are randomly selected, and the best one transfers its knowledge to the other student. Eq.(3) is used for mathematical emulation:

$$L_i^{new} = L_i^{old} + r_i\,(L_i^{old} - L_j^{old}) \quad if \quad f\,(L_i^{old}) < f\,(L_j^{old}) \,(3)$$

In the above equation, L_i is for solution and $f(L_i^{old})$stands for its fitness value. At the end of each phase, replacement has occurred if $f(L_i^{new})$is better than $f(L_i^{old})$. The flowchart of the GT-TLBO in Fig. 2 indicates the proposed method of choosing the best and the most correct cyber configuration satisfying cyber protocols with minimum EENS index for maximizing cyber-power reliability.

D. *Function evolution(EENS assessment)*

The in-service and out-service probability of each power system element are significant parameters for evaluating the adequacy of systems. To emulate this, it is necessary to identify up-time variables of the element and down-time of the element corresponding to in-service and out-service, respectively [16-18]. Calculation of up-time and down-time of each element can be also performed using Eq.(4) and Eq.(5). In this equation, illustrating two-state reliability model concept, mean time to failure (MTTF) and mean time to repair (MTTR) are inherent features of each element. In this respect, uniform random variables (*u_1&u_2*) distributed on [0- 1] are required to calculate this exponential distribution model which produces up and down states of each element. MTTR and MTTF are also proprietary parameters of each element obtained from historical element data. Within this reliability method, 24 hours of a day for each element should be cleaved to some up-time and down-time zones as shown in Fig. 1. Given the nature of the stochastic method, these zones should be created randomly through uniform random variables (u1&u2) distributed on [0- 1].

$$Up - time_j = -MTTF_j \times Ln\left(u_1\right) \qquad (4)$$

$$Down - time_j = -MTTR_j \times Ln\left(u_2\right) \qquad (5)$$

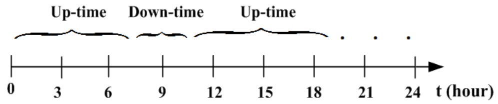


Fig. 1. Random up-times and down-times of the element during 24 hours of the day according to the historical data.

The availability parameter that shows an element is in service or out of service in each time zone (an hour of the day) within Monte Carlo simulation should be calculated for each element; wherein *availability (j,t)* is the variable that shows ^{jth} element is in-service or out-service in a power system. If *availability (j,t)* is one, it means that ^{jth} element serves the system; and if *availability (j,t)* is zero, it means that ^{jth} element does not serve the system.

$$availibilty\,(j\,,t\,) = \begin{cases} 1 & t \in Up - time_j \\ 0 & t \in Down - time_j \end{cases} \qquad (6)$$

$$S\,(t\,) = \left[s\,(1,t\,),\dots,s\,(N_P\,,t\,)\right] \qquad (7)$$

S(t) stands for total availability of the whole elements indicating each element is in-service or out-service within each time segment of simulation. Finally, given the state of the entire power system elements and considering electricity network power balance along with power flow calculation and other system limitations, the expected energy not supplied (EENS) as one of the best adequacy indices could be calculated. The Monte Carlo simulation for EENS evolution are explained with more details in [19-21].

It should be mentioned that recently Jaya algorithm has been introduced by R. Rao [22]. Jaya algorithm has the advantages of TLBO algorithm and it is simpler to apply compared to TLBO [23]. Authors of this paper will use the Jaya algorithm in their future works.

V. IMPORTANCE OF GT-TLBO FOR WIDE CYBER NETWORK

Although choosing the best cyber configuration in small cyber networks is simple and it can be done through trial and error such as those reported in previous works and cyber network is wide with lot of devices; thus, an appropriate algorithm must be used by computer for searching its best configuration. In this respect, simple methods like trial and error by human are not applicable.

If power network is wide, a complicated cyber network system is needed for its monitoring and controlling. For *n*th

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TII.2018.2860984, IEEE Transactions on Industrial Informatics

devices of cyber-network system, Eq.(8) illustrates the relation between different devices of this cyber network system in which p, q, r refer to the numbers of servers, EMUs, and switches; respectively.

$$p+q+r=n \tag{8}$$

GT-TLBO algorithm selects proper configuration of the cyber network using the following steps:

1) Initializing $n\times n$ adjacency matrix of the cyber network.

2) Checking Kosaraju's DFS-based algorithm on adjacency matrix of the cyber network (first constraint).

3) Checking Dijkstra algorithm on adjacency matrix of the cyber network (second constraint).

4) Implementing TLBO process on adjacency matrix of the cyber network appropriate for optimization goals.

5) Converting the final adjacency matrix of the cyber network into its graph configuration.

Using the proposed method, choosing an appropriate cyber-network system is not frightening for a large power network and it can be done according to each specific goal. If the aggregated cyber-network system is needed for monitoring and controlling several cities as one bulk power system, this novel method is highly applicable by doing GT-TLBO on adjacency matrix of the aggregated cities.

In the first step, $n\times n$ adjacency matrix of the cyber network should be initialized in TLBO algorithm. The number of design variables is $\frac{n^2-n}{2}$ because the adjacency matrix is symmetric matrix and the elements of main diagonal of this matrix is zero . The maximum and minimum limits of design variables are 0 and 1, respectively. The value of variables should be rounded because of zero-one nature of adjacency matrix. Fig. 2 demonstrates the design variables of adjacency matrix in TLBO algorithm.

$$\begin{bmatrix} 0 & & & & & & \\ X_1 & 0 & & & & & \\ X_2 & X_3 & 0 & & & & \\ . & . & . & . & & & \\ . & . & . & . & . & & \\ . & . & . & . & . & 0 & \\ X_{\frac{n^2-n}{2}-n+1} & . & . & . & . & X_{\frac{n^2-n}{2}} & 0 \end{bmatrix}_{n\times n}$$

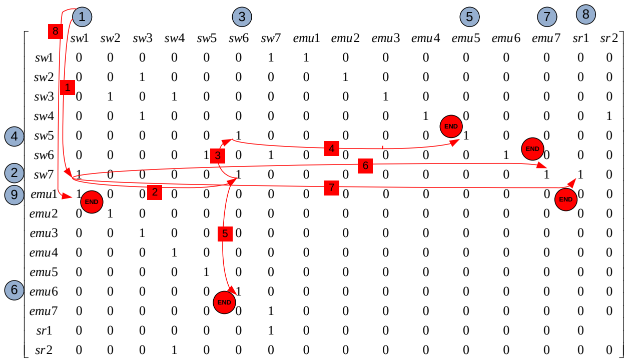
Fig. 2. Design variables of adjacency matrix in TLBO algorithm

For better understanding of GT-TLBO procedures, the following example is explained. Assume that the sample power network needs the cyber network with 7 switches, 7 EMUs and 2 servers. The problem is that which cyber graph can satisfy the cyber protocols and has minimum EENS in relation to power network. The proposed GT-TLBO can solve this problem as follows:

In this problem, the number of elements is 16 and according to variables of adjacency matrix $(\frac{n^2-n}{2})$, the number of design variables is 120. One of the random adjacency matrices of this cyber network that is produced by TLBO algorithm is shown in fig. 3. Now the protocols of cyber network should be checked by the Kosaraju's DFS and Dijkstra algorithms. Fig. 4 illustrates the procedures of Kosaraju's DFS on the adjacency matrix. In the Kosaraju's DFS algorithm, the matrix is acceptable if all nodes are connected to each other. In the first step, switch1 is chosen randomly, marked and counted, then neighbors of switch1 (switch7 and EMU1) are marked and counted. The neighbors of marked varices should be marked and counted aging until all the neighbors of all marked vertices are marked. The red square shows number of steps of this algorithm. In this matrix, the number of counted vertices (9) is less than the total number of vertices (16), so Kosaraju's DFS algorithm is not true and this random adjacency matrix is not acceptable. Although this matrix is not valid, for better understanding of the graph theory procedure, validity of the second algorithm is studied for this matrix in Fig. 5 and Fig. 6. The matrix is acceptable in Dijkstra algorithm if each EMU is connected to at least one server. In Fig. 5 and Fig.6, EMU 5 is studied as origin and server1 and servere2 are studied as destinations, separately. In Fig, 5, EMU 5 is selected and marked and then its neighbors are marked too. Neighbors of marked vertices should be marked aging until all neighbors of all marked vertices are marked. In the end of the process, the Dijkstra algorithm is true for EMU 5 if the server1is marked. The process is repeated for EMU 5 as origin and server 2 as destination in Fig. 6. The Dijkstra algorithm is true because EMU 5 as origin is connected to at least one server (server1) as destination. Dijkstra process should be studied for each EMU. If Dijkstra is true for each eum, the Dijkstra is true for the matrix. For this sample matrix, Dijkstra is true. If Kosaraju and Dijkstra are true for each randomly produced matrix, the matrix is valid for EENS assessment. The TLBO algorithm chooses the valid matrix with minimum EENS. Fig. 7 shows the graph of this sample cyber network.

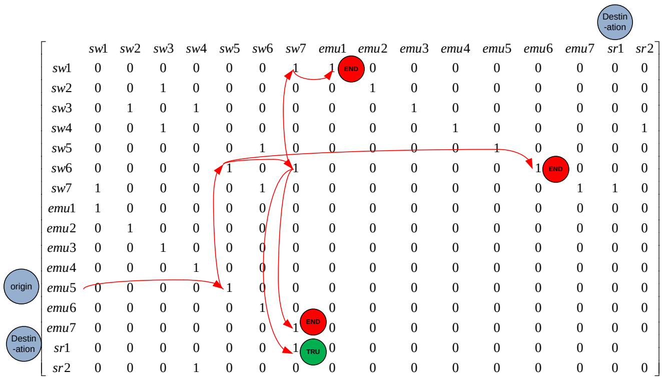
	*sw*1	*sw*2	*sw*3	*sw*4	*sw*5	*sw*6	*sw*7	*emu*1	*emu*2	*emu*3	*emu*4	*emu*5	*emu*6	*emu*7	*sr*1	*sr*2
*sw*1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
*sw*2	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
*sw*3	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0
*sw*4	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1
*sw*5	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
*sw*6	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0
*sw*7	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0
*emu*1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
*emu*2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
*emu*3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
*emu*4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
*emu*5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
*emu*6	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
*emu*7	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
*sr*1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
*sr*2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 3. Adjacency matrix of sample cyber network that is produced by TLBO



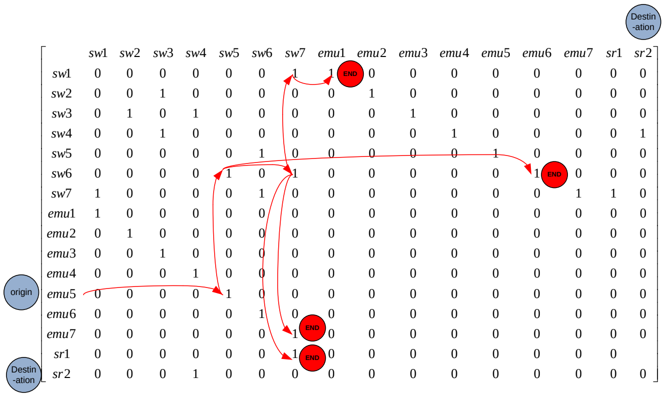
	*sw*1	*sw*2	*sw*3	*sw*4	*sw*5	*sw*6	*sw*7	*emu*1	*emu*2	*emu*3	*emu*4	*emu*5	*emu*6	*emu*7	*sr*1	*sr*2
*sw*1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
*sw*2	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
*sw*3	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0
*sw*4	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1
*sw*5	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
*sw*6	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0
*sw*7	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0
*emu*1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
*emu*2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
*emu*3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
*emu*4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
*emu*5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
*emu*6	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
*emu*7	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
*sr*1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
*sr*2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 4. Process of Kosaraju DFS based algorithm in the sample cyber network



	sw1	sw2	sw3	sw4	sw5	sw6	sw7	emu1	emu2	emu3	emu4	emu5	emu6	emu7	sr1	sr2
sw1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
sw2	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
sw3	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0
sw4	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1
sw5	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
sw6	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0
sw7	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0
emu1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
emu2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
emu3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
emu4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
emu5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
emu6	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
emu7	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
sr1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
sr2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 5. Process of Dijkstra algorithm for EMU 5 as origin and server1 as destination in the sample cyber network.



	sw1	sw2	sw3	sw4	sw5	sw6	sw7	emu1	emu2	emu3	emu4	emu5	emu6	emu7	sr1	sr2
sw1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0
sw2	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0
sw3	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0
sw4	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	1
sw5	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0
sw6	0	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0
sw7	1	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0
emu1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
emu2	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
emu3	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
emu4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
emu5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
emu6	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
emu7	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
sr1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	
sr2	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0

Fig. 6. Process of Dijkstra algorithm for EMU 5 as origin and server2 as destination in the sample cyber network.

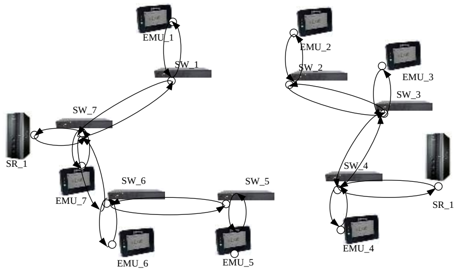


Fig. 7. Graph of sample cyber network

Each bulk cyber network with n elements can be studied in this GT-TLBO algorithm for selecting the best configuration. The cyber protocols are not formulated and studied in the previous works, so selecting the best configuration is not possible for any n-th cyber elements and bulk power systems.

VI. Test Results

The 20kV distribution system of Hormozgan Regional Electric Company (HREC) in tropical southeastern part of Iran was studied for applying this novel method. Four transformers had been supplied in the main sub-station of this case study. Fig.7 shows three protective devices in buses 1, 17 and 27 that had made three segments with an aggregated peak load of 1.8MW, 1.3MW and 2.9 MW; respectively. Segment failures were also respectively considered by 0.2057% and 0.587%, which were taken from the historical data of this feeder. Mean time to failure (MTTF) and mean time to repair (MTTR) of power elements were also determined as reported in [24, 25].

DG unit locations consisting of PV-based DG unit, wind turbine-based DG unit, and diesel-based DG units were shown in fig. 8, and the characteristic data of different DG technologies were illustrated in Table I.

According to the power network, the cyber network needs 5 switches, 5 EMUs and 2 servers. Cyber network has 12 elements and the number of design variables is 66. The number of population and the number of iteration are set as 70 and 120, respectively. The computation time for choosing the best configuration of this case is about 48 minutes. The reasons of long computation time are the Monte Carlo simulation for EENS evaluation, Kosaraju's DFS and Dijkstra checking for each student and number of population and iteration. It should be mentioned that design variables of students should be rounded to 0 or 1 in each step of TLBO algorithm.

It should be noted that different connections of the cyber system have various power reliability values due to cyber-power relation. Fig.8. shows the power system and the proposed configuration of the cyber system with maximum reliability according to the graph theory and TLBO optimization. Purple dash lines in this figure display the relation between each EMU in the cyber network with their DG units in the power system to control and collect data from them. Bi-directional lines in Fig 3 illustrate the two-way flow of information. This system has five EMUs, five switches, two servers, and eleven pairs of connection wires. EENS as an important reliability index was equal to 42.91 MW annually for the best cyber configuration of the proposed GT-TLBO method. Table II shows the importance of the proposed method compared with those in previous studies. This Table reveals how EENS had decreased in this paper compared to configurations in [3] and [4]. All the references have identical conditions with different cyber configurations. In addition to filling the knowledge gap of choosing the best configuration for cyber-network system within wide and complicated networks by the GT-TLBO algorithm, its advantages of selecting the best configuration for the simpler cyber- network system compared with those used in previous papers are clarified.

TABLE I
Capacity and Controller of Different DG Technologies

DG	Capacity	Cyber controller
Diesel_1	900kW	EMU_1
Diesel_2	900kW	EMU_2
Diesel_3	900kW	EMU_3
PV	900kW	EMU_4
Wind turbine	900kW	EMU_5

TABLE II
Comparison of EENS between cyber configurations of this paper and references[3] and [4]

Method	EENS
This paper	42.91 MW
Reference[3] in best configuration	53.70 MW
Reference [4]	61.32 MW

Different configurations of a cyber-network system and their GT-TLBO characteristics are investigated in Table III.

Configuration No. 1 was not continuous and an EMU was not connected to servers, so Kosaraju law and Dijkstra law were not met and the configuration was not acceptable. In configuration No. 2, continuity was not satisfied; but each EMU was connected to servers in small routes. For this configuration, the EENS criteria were not calculated.

Although continuity was satisfied in configuration No. 3, the existence of the shortest route between EMUs and servers was not verified. When Dijkstra law was confirmed in the given configuration, the time of data analysis in the cyber network and the probability of the mistake in data flow decreased. So, it is necessary to meet the Dijkstra law in the configuration to reach the best one. Kosaraju and Dijkstra laws were met in configurations No. 4, 5, and 6; but different EENS were separate from each other. The last configuration had the smallest EENS due to TLBO analysis and the reliability of power network was reported to be at the highest level. In this case, annual EENS was 42.91 MW and its minimum was accessible.

VII. Conclusion

In this paper, a novel method was proposed to introduce the optimized reliable configuration for any of the *n*th devices of a cyber-network system having a direct relation with the power system. For this purpose, two concepts were considered; the first concept was graph theory for the confidence level of connectivity of cyber system and the existence of at least one route between each switch and server to confirm the cyber protocols, and the second one was teaching-learning-based optimization to calculate the EENS of each cyber configuration and to choose the best one for more reliability. The results revealed that the proposed method was applicable for every bulk power system and EENS indices had been improved compared with those reported in previous studies on cyber-network systems. This method has many advantages such as decreasing blackout and increasing economic benefits.

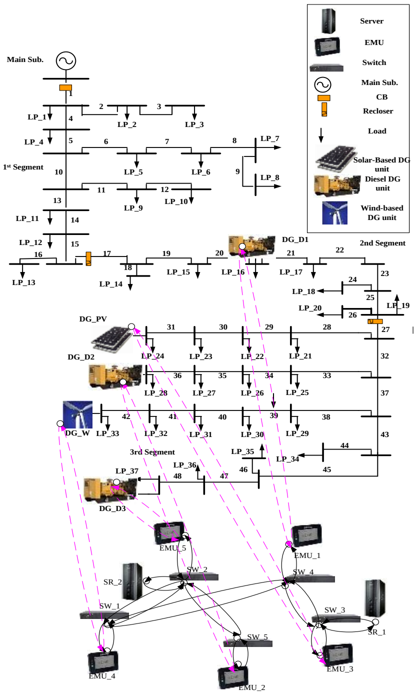
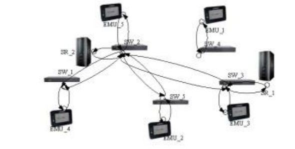
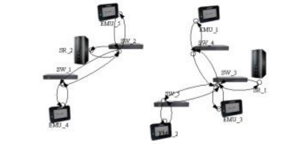
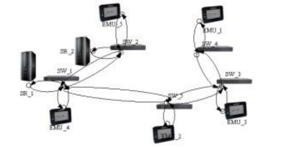
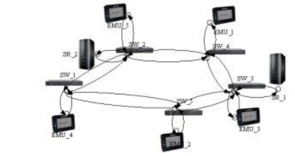
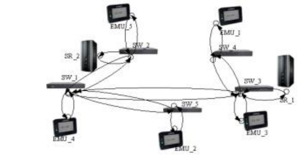
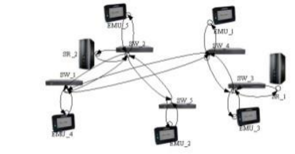


Fig. 8. Proposed configuration of cyber system for maximized reliability of power system considering TLBO-GT algorithm

TABLE III
COMPARISON OF EENS BETWEEN CYBER CONFIGURATIONS OF-THIS SYSTEM

N.O.	Configuration	Kosaraju	Dijestra	EENS from TLBO
1		No	No	–
2		No	Yes	–
3		Yes	No	–
4		Yes	Yes	55.30
5		Yes	Yes	48.65
6		Yes	Yes	42.91 (best)

REFERENCES

[1] M. McGranaghan, D. Von Dollen, P. Myrda, and E. Gunther, "Utility experience with developing a smart grid roadmap," in Proc. IEEE PES Gen. Meet., 2008, Jul. 20-24, 2008, pp. 1-5.

[2] M. G. Adamiak, A. P. Apostolov, M. M. Begovic, C. F. Henville, K. E. Martin, G. L. Michel, A. G. Phadke, and J. S. Thorp, "Wide area protection-Technology and infrastructures," IEEE Trans. Power Del, vol. 2, no. 2, pp. 601-609, Apr. 2006.

[3] H. H. Dezaki, M. M. Agah, H. A. Abyaneh and H. Haeri, "Sensitivity analysis of smart grids reliability due to indirect cyber-power interdependencies under various DG technologies, DG penetrations, and operation times," Energy convers Manage., vol. 108, pp. 377–391, May 2016.

[4] B. Falahati, Y. Fu and L. Wu, "Reliability Assessment of Smart Grid Considering Direct Cyber-Power Interdependencies," in IEEE Transactions on Smart Grid, vol. 3, no. 3, pp. 1515-1524, Sept. 2012.

[5] B. Falahati, Y. Fu, "Reliability assessment of smart grids considering indirect cyber-power interdependencies", IEEE Transactions on Smart Grid, vol. 5, no. 4, pp. 1677-1685, July 2014.

[6] H. H. Dezaki, H. A. Abyaneh and H. Haeri, "Impacts of direct cyber-power interdependencies on smart grid reliability under various penetration levels of microturbine/wind/solar distributed generations," IET-GTD., vol. 10, pp. 928 - 937, March 2016.

[7] E. Moradi-Pari, N. Nasiriani, Y. P. Fallah, P. Famouri, S. Bossart and K. Dodrill, "Design, Modeling, and Simulation of On-Demand Communication Mechanisms for Cyber-Physical Energy Systems," in IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2330-2339, Nov. 2014.

[8] T. Facchinetti and M. L. Della Vedova, "Real-Time Modeling for Direct Load Control in Cyber-Physical Power Systems," in IEEE Transactions on Industrial Informatics, vol. 7, no. 4, pp. 689-698, Nov. 2011.

[9] R. Liu, C. Vellaithurai, S. S. Biswas, T. T. Gamage and A. K. Srivastava, "Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid," in IEEE Transactions on Smart Grid, vol. 6, no. 5, pp. 2444-2453, Sept. 2015.

[10] D. B. West, " Introduction to Graph Theory,", Second Edition, Prentice Hall, Inc., Upper Saddle, River, NJ, 2001.

[11] J.A., Bondy, U.S.R , Murty, " Graph Theory,", Graduate Texts in Mathematics, vol. 244. Springer, New York, 2008.

[12] Micha Sharir. "A strong connectivity algorithm and its applications to data flow analysis". Computers and Mathematics with Applications 7(1):67–72, 1981

[13] W. E. Dijkstra, "A note on two problems in connexion with graphs," Numerische Mathematik, vol.1 PP. 269–271, 1959.

[14] R. Rao, V. Savsani, and D. Vakharia, "Teaching–learning-based optimization: an optimization method for continuous non-linear large scale problems," Inf. Sci. (Ny), vol. 183, no.1,pp. 1-15,Jan. 2012.

[15] R.V. Rao, Teaching Learning Based Optimization Algorithm: And Its Engineering Applications, 1st ed., Springer Publishing Company, Incorporated, 2015.

[16] R. Billinton and R. Karki, "Reliability/cost implications of PV and wind energy utilization in small isolated power systems," IEEE Trans. Energy Convers., vol. 16, no. 4, pp. 368–373, Dec. 2001.

[17] Y. M. Atwa, E. F. El-Saadany, M. M. A. Salama, R. Seethapathy, M. Assam, S. Conti, "Adequacy evaluation of distribution system iIncluding wind/solar DG during different modes of operation," IEEE Trans. Power syst., vol. 26, no. 4, pp. 1945-1952, Nov. 2011.

[18] Forooghi Nematollahi A, Dadkhah A, Asgari Gashteroodkhani O, Vahidi B. Optimal sizing and siting of DGs for loss reduction using an iterative-analytical method. Journal of Renewable and Sustainable Energy. 2016 Sep;8(5):055301.

[19] Y.M. Atwa, E.F. El-Saadany, A.C. Guise, "Supply adequacy assessment of distribution system including wind-based DG during different modes of operation", IEEE Trans. Power Syst., vol. 25, no. 1, pp. 78-86, Feb. 2010.

[20] Jikeng L, Xudong W, Ling Q. Reliability evaluation for the distribution system with distributed generation. Eur Trans Electr Power 2011;21(1):895–907.

[21] Billinton R, Karki B. Well-Being analysis of wind integrated power systems.IEEE Trans Power Syst 2011;26(4):2101–8.

[22] R. Rao, Jaya: A simple and new optimization algorithm for solving constrained and unconstrained optimization problems, International Journal of Industrial Engineering Computations 7 (1) (2016) 19–34.

[23] R. Rao, K. More, J. Taler, and P. Oclon, Dimensional optimization of a micro-channel heat sink using jaya algorithm, Applied Thermal Engineering 103 (2016), pp. 572 – 582.

[24] M. Hamzeh, B. Vahidi and H. Askarian-Abyaneh, " Reliability evaluation of distribution transformers with high penetration of distributed generation," International Journal of Electrical Power & Energy system, vol. 73, no.1,pp. 163-169, Dec. 2015.

[25] M. Hamzeh, H. H. Dezaki, H. A. Abyaneh, G. B. Gharehpetian, B. Vahidi, " Risk management of smart grids based on plug-in hybrid electric vehicles' charging considering transformers' hottest spot temperature-dependent aging failures," Renewable and Sustainable Energy, vol. 8, no. 3, pp. 034102- 034132, 2016.

Mohsen Hamzeh was born in 1990, Kashan, Iran. He received B.S. & M.S degrees in electrical engineering from Amirkabir University of Technology, Tehran, Iran in 2013 & 2015. Presently, he is a PhD. student at the department of electrical engineering of Amirkabir University of Technology, Tehran, Iran. Also he is visiting Ph.D. student at Politecnico di Milano, Milan, Italy. His main fields of research are smart grids, power system reliability, cyber system and transformers.

Behrooz Vahidi was born in Abadan. He received the B.S. in electrical engineering from Sharif University of Technology, Tehran, Iran in 1980 and M.S. degree in electrical engineering from Amirkabir University of Technology, Tehran, Iran in 1989. He also received his Ph.D. in electrical engineering from UMIST, Manchester, UK in 1997. From 1980 to 1986 he worked in the field of high voltage in industry as chief engineer. From 1989 to present he has been with the department of electrical engineering of Amirkabir University of Technology where he is now a professor. He has authored and co-authored more than 400 papers and 6 books on high voltage engineering and power system.

Amin Foroughi Nematolhahi was born in Iran in 1991. He received the M.S. degree in electrical engineering from Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran, in 2016. He is currently working toward the Ph.D. degree at High Voltage Laboratory, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran. His current research interests include planning problems of distribution networks, Optimization and Power Systems Transients.