Recovery of Structural Controllability into Critical Infrastructures under Malicious Attacks

Bader Alwasel
Department of Applied Natural Sciences, Computer Science
Unaizah Community College
Qassim University
Saudi Arabia

***Abstract*—The problem of controllability of networks can be seen in critical infrastructure systems which are increasingly susceptible to random failures and/or malicious attacks. The ability to recover controllability quickly following an attack can be considered a major problem in control systems. If this is not ensured, it can enable the attacker to create more disruptions as well as, like the electric power networks case, violate real-time restrictions and result in the control of the network degrading and its observability reducing significantly. Thus, the present paper examines structural controllability problem that has been in focus through the equivalent problem of the Power Dominating Set (PDS) introduced in the context of electrical power network control. However, the controllability optimisation problem can be seen as computationally infeasible regarding large complex networks because such problems are considered NP-hard and as having low approximability. Hence, the ability of structural controllability recoverability will be explored as per the PDS formulation, especially following perturbations in which an attacker with sufficient knowledge of the network topology is only able to completely violate the current driver control nodes of the original control network leading to a degradation of controllability of dependent nodes. The results highlight that the use of directed Laplacian matrix can be a useful approach for analysing structural controllability of a network. The simulation results show also that an increase of a connectivity probability of the distribution of links in Directed ER networks can minimise the number of driver control nodes which is highly desirable while monitoring the entire network.**

***Keywords*—Structural controllability; control systems; cyber physical systems; power dominating set; recovery from attacks**

I. Introduction

Securing control systems have attracted significant attention to many researchers from various fields [1]. Random failures or malicious attacks can turn critical infrastructure components' pairwise dependencies uncontrollable, leading to severe economic effects. Hence, it is important to effectively assess all pairwise dependencies among components to keep control into infrastructures and protect critical infrastructures. Further, domination, which is a significant subject in graph theory, can be regarded as a crucial theme in the control systems' design and analysis as it is similar to the (Kalman) controllability problem. It is the concept of structural controllability, as introduced by Lin [2], that provides the motivation and presents a graph-theoretical interpretation in terms of control systems which was first put forth Kalman [3].

$$\dot{x}(t) = \mathbf{A}x(t) + \mathbf{B}u(t), \qquad x(t_0) \ = \ x_0 \tag{1}$$

In this equation, $x(t) = (x_1(t), \ldots, x_n(t))^T$ the current state of a system with n nodes at time t, a $n \times n$ adjacency matrix $\mathbf{A}$ representing the network topology of interactions among nodes, and $\mathbf{B}$ the $n \times m$ input matrix ($m \leq n$), identifying the set of nodes controlled by a time-dependent input vector $u(t) = (u_1(t), \ldots, u_m(t))$ which forces the desired state. According to Kalman's rank criterion, the system in equation (1) is controllable if and only if:

$$\text{rank } [\mathbf{B}, \mathbf{AB}, \mathbf{A}^2\mathbf{B}, \ldots, \mathbf{A}^{n-1}\mathbf{B}] = n \tag{2}$$

On the other hand, large networks such as power networks or even large control systems find it prohibitively expensive to affirm this criterion as there is a computational difficulty in verifying all possible combinations concerning large complex networks. This because the number of input combinations increases exponentially as per the number of nodes. Lin's graph-theoretical interpretation concerning Kalman's algebraic criterion was a major contribution that enabled the required and adequate conditions to be determined for identifying individual Driver Nodes (denoted as N_D). Such driver control nodes can control a system that has a particular structure (topology). The system in Eq. (1), denoted by $(\mathbf{A}, \mathbf{B})$, can be interpreted as the matrix $\mathbf{A}$ giving the network topology, and the matrix $\mathbf{B}$ can be interpreted as the set of nodes with the capacity to drive control.

Lin [2] gives the interpretation of $G(\mathbf{A}, \mathbf{B}) = (V, E)$ as a digraph where $V = V_{\mathbf{A}} \cup V_{\mathbf{B}}$ the set of vertices and $E = E_{\mathbf{A}} \cup E_{\mathbf{B}}$ the set of edges. In this representation, $V_{\mathbf{B}}$ comprises nodes able to inject control signals into the entire network, also known as Driver Nodes (N_D) corresponding to input vector u in Equation (1). In control systems, being able to determine driver control nodes is vital for attackers as well as defenders. For identifying the minimum number of driver node subsets, various methods can be used for determining N_D; however, the Maximum Matching approach [4] has been focused on the most. This approach by Liu *et al*. is based on a non-rigorous variant of the Maximum Matching problem to identify a subset of N_D. This paper studies an alternative approach following the Power Dominating Set (PDS) problem that was proposed by Haynes *et al*. [5] as a model for studying electric power networks as well as an extension to the well-known Dominating Set (DS) problem. Through the PDS approach, an equivalent formulation can be obtained to determine the minimum N_D. This interest is mainly based in the real-world context because of the significant similarities between the logical structures of PDS-based networks and the real-world monitoring systems, in

which driver nodes can represent e.g. control terminal units that control industrial sensors or actuators. The recovering strategy presented in this paper focuses on sparse Erdős-Rényi with directed control edges that provides similar aspects to real power networks. This recovering strategy seeks to control a network after a threat in which an attacker can compromise a subset of driver control nodes, leading to the breakdown of the network into pieces and damage the control network.

The remainder of the paper is structured as follows. Section II presents the related work and network controllability considering vulnerability. Section III discusses the initial assumptions as well as conditions that were taken into account for recovering structural controllability when there were adversaries positioned within a network to attack critical nodes. Section IV introduces a new optimal recovering strategy for repairing structural controllability after perturbations as per the PDS formulation while Section V analyses the computational complexity of recovering algorithm; followed by the simulation results for repairing structural controllability. Section VI, we close this paper with some conclusions.

II. Power Domination and Related Work

The study of the PDS problem with respect to the graph-theoretical representation was initiated by Haynes *et al*. [5] as a model for studying electric power networks and their efficient monitoring as an extension to the well-known Dominating Set (DS) problem. As shown by the authors of [5], PDS for a particular graph G is **NP**-complete in terms of general graphs despite being reduced to specific classes of graphs, such as chordal graphs and bipartite graphs. Guo *et al*. [6] showed that the PDS problem is also **NP**-complete for planar graphs, circle graphs, and split graphs, and it cannot be better approximated than the domination problem for general graphs. Further, [6], [7] presented parametrised results and proved $W[2]$-hardness in case of the parameter's size being equal to that of the solution through decreasing a DS to a PDS. Guo *et al*. [6] also presented fixed-parameter tractability of PDS regarding a tree decomposition of bounded tree-width for the underlying graph. A concrete algorithm that can turn PDS into an orientation problem on undirected graphs was developed by [6]. Considering the fact that the PDS problem is the dominating set problem's generalisation, the basic minimum DS problem is known to be **NP**-complete with a polynomial-time approximation factor of $\theta(\log n)$ as noted by Feige [8]. Hence, Aazami and Stilp [9] differentiated between the approximation hardness of DS and PDS problems and verified that it is not possible to better approximate the PDS problem than $2^{\log^{1-\epsilon} n}$, unless $\mathbf{NP} \subseteq DTIME(n^{polylog(n)})$. They also presented an $O(\sqrt{n})$-approximation algorithm for the PDS problem in planar graphs. Liao and Lee [10] showed a different **NP**-completeness proof for the PDS problem in split graphs as well as introduced a polynomial-time algorithm for solving PDS optimally on interval graphs. As shown by Binkele-Raible and Fernau, the PDS problem continues to be **NP**-hard on cubic graphs[11]. Guo *et al*. [6] also presented valid orientations to optimally address PDS on undirected graphs having bounded tree-width. Furthermore, the Directed PDS (DPDS) was reformulated by Aazami and Stilp [12] as Valid Colourings of edges, and they developed a dynamic programming algorithm concerning a DPDS in which the underlying undirected graph had bounded tree-width. The previous work on PDS in different graph classes examined and determined that such structures could be embedded in Erdős-Rényi graphs having varied density and approximation characteristics [13]. This can help to implement the ideas involved in addressing the PDS problem. An algorithm was also developed for decreasing a reconstruction algorithm's average-case complexity for (directed) control graphs through the re-use of the rest of the original graph' fragments wherever they could be re-used [14]. Also, it detects edges that were previously un-used for reducing the number of PDS.

A. Network Controllability under Attack

Certain network vertices experiencing malfunctioning because of malicious attacks or random failures can lead to the entire network breaking down into isolated parts. The authors of [15] studied the attack vulnerability of network controllability for the canonical model networks according to five different strategies subject to attacks on nodes and edges. In terms of Erdős-Rényi random graph, especially directed graphs, *et al*. [16] presented the most significant study by examining the controllability of directed Erdős-Rényi as well as scale-free networks when facing single-node attack along with cascading failure attack. They also noted that the degree-based attacks in directed Erdős-Rényi and scale-free networks have a greater impact on network controllability compared to random attacks. They further noted that network controllability can be adversely impacted by cascade failures, despite a local node failure being induced. In addition, the effects of vertices being removed from different networks were studied according to six complex networks' attack vulnerability which included Erdős-Rényi model of random networks [17]. This study also noted that, as against the original network-based attack strategies, there were more detrimental impacts of elimination through the recalculated degrees and betweenness centralities. Moreover, the Erdős-Rényi random digraph's structural controllability was also assessed while the question of recovering a control graph to a large extent was explored in case of the PDS or its dependent nodes being infringed upon partly without complete re-computation [18]. The same method was implemented by Alcaraz *et al*. [19] for recovering the precise scale-free networks' structural controllability following nodal removal. Further, in [20], how various non-interactive attack types impact the PDS as well as how underlying graphs affect numerous network topologies were evaluated. Barthlemy [21], on the other hand, examined the importance of the nodes' betweenness centrality in Erdős-Rényi and scale-free networks in which eliminating betweenness centrality of nodes leads to new disconnected components. Liu *et al*. [22] investigated the single node's control centrality in complex networks including directed Erdős-Rényi random graph. They also showed that upstream (or downstream) neighbours selected randomly involve a higher proportion of outgoing (or incoming) links compared to the node. The authors of [23] studied the possibility to recover the structural controllability of the residual system with a minimum set of inputs without re-computation. They also proposed an efficient algorithm to classify each network single vertices in order to maintain the current minimum number of inputs [24].

III. Conditions for the Analysis

This section discusses the initial assumptions as well as conditions implemented for recovering structural controllability when adversaries are in position within a network for attacking the driver control nodes. Let $G(V,E)$ be a directed graph, constructed as $ER(n,p)$, with an arbitrary set of nodes V and a set of edges E. Each edge included in the graph is determined independently with probability p. In this paper, we consider only the resulting instance of $ER(n,p)$ that is connected without its isolated vertices. Any ordered pair of vertices $v_i, v_j \in V(G)$ is connected with p by a directed edge $e = v_i, v_j \in E(G)$ without producing self-loops or parallel edges, but may have two edges with different directions on the same two end vertices (called anti-parallel edges).

A. Assumptions for Perturbation

Here, the first assumption is that one or multiple adversaries who are knowledgeable about the network distribution, its topology, or its power domination relation, and the identities of the current driver control nodes N_D can compromise the N_D properties. These driver nodes that also belong to V satisfy the two observation rules for controllability defining by two rules, simplified by Kneis *et al*. [7] from the original formulation by Haynes, *et al*. [5]:
[OR1] A vertex in N_D observes itself and all of its neighbours.
[OR2] If an observed vertex v of degree $d \geq 2$ is adjacent to $d-1$ observed vertices, then the remaining unobserved neighbour becomes observed as well.

As this paper focuses on the problem of structural controllability for directed networks, here we consider a straightforward extension to directed networks for identifying minimum driver node subsets. To identify the minimum driver node subsets N_D, we follow the approach based on the PDS problem, which is described in more detail in [5] (note that the PDS problem gives an equivalent formulation for identifying minimum driver node subsets). The construction of N_D depends on choosing vertices that fulfil **OR1** and such N_D can control all vertices in $V \setminus N_D$ through utilising **OR2**. Note that PDS differs from DS problem only by the inclusion of **OR2**, and DS (and hence PDS) are known to be **NP**-complete for general graphs; PDS is $W[2]$-hard and only $\Theta(\log n)$ approximable for general graphs [8]. This paper endeavours to further explore the occurrence of the scenarios given below and develop a recovering strategy that can repair the controllability

SCENARIO: After attaining N_D for a given network, it is assumed that an attacker having thorough knowledge concerning the structure of the network and its N_D can compromise the set N_D as well as its dependent nodes through violating the configuration of N_D from the network and then disrupting the network control.

Hence, this attack scenario may as in the case of electric power networks result in leading to significant loss of control of a network or temporary loss of observability as well as partial observability. For resolving this problem concerning the PDS formulation, overall controllability should be recovered by complete re-computation of the N_D structure under the above type of the attack leading to the N_D properties getting violated.

B. Assumptions for Recovery

There are several assumptions being depended on for recovering structural controllability of a compromised N_D. For recovering controllability it is important for the candidates in N_D to possess the following properties :

- Fulfil the constraint of **OR1** by selecting an $n_d \in N_D$ that can observe itself as well as an unobserved $u \in U$ using a new link $(n_d, u) \in E$ such that $|N_D| \geq 1$.
- Confirm that the candidate n_d does not breach the observation rule **OR2**

Note that although the ability to minimise the candidate driver nodes is highly desirable while recovering the controllability of a network, the driver nodes obtained may increase such that in the worst case $|N_D| = |V|$. It is also important, however, to take into account the handicap of non-locality of PDS as well as the **NP**-complete property presented by Haynes *et al*. [5].

IV. Recovery of Structural Controllability

The Laplacian matrices of graphs are fundamental to represent the network topology and is a useful approach for analysing network structure. To ensure that the observation rules given in Section III are satisfied while recovering structural controllability of a given compromised network, the following approaches are considered when designing the algorithm:

- **APPR-1** Find the adjacency matrix $A(G)$ of a given network G such that the $m \times n$ matrix whose entries a_{ij} are given by

$$a_{ij} = \begin{cases} 1 \text{ if there is outgoing edge } (v_i, v_j) \in E \\ 0 \text{ otherwise.} \end{cases}$$

- **APPR-2** Find the out-degree matrix for G, denoted by $D(G)$, where for every node $v \in V$, the out-degree $d(v)$ of v is the number of edges leaving v such that $v : d(v) = |u \in V | (v,u) \in E \ \ or \ \ (u,v) \in E|$.

After **APPR-1** and **APPR-2** are obtained, the following two recovering rules should be considered to select the best candidate in N_D such that the two observation rules **[OR1]** and **[OR2]** specified above are satisfied, which are the basic constraints to address the recovery strategy.

- **RR1:** Determine a vertex having maximum out-degree, providing the controlling of unobserved nodes in the set of unobserved nodes U.
- **RR2:** In case of equality in out-degree, an initial vertex should be selected randomly, offering the coverage of unobserved nodes in U.

A. Recovering Algorithm and Analysis

For the attack scenario given in Section III, the approach involves finding the driver candidates N_D that can provide coverage to control each vertex contained in a given network after N_D has been perturbed. The correctness proof of the approach is provided including induction:

The first phase (PHASE-1) is to initialise a set of unobserved vertices U of the entire graph G and then, present the

directed Laplacian matrix of G (**APPR-1**). After the out-degree matrix $D(G)$ is obtained satisfying the first recovery restoration condition (**RR1**) given above, a vertex $v \in U$ having maximum out-degree is determined, and then a verification process is performed to ensure that v does not include the set N_D. If the obtained vertex satisfies the first observation rules **OR1** which observes itself and all of its children, then $v \in N_D$ is added to the set N_D, and only after that the set N_D and the observed vertices, denoted by O is updated, guaranteeing that U is updated to apply the second observation rules **OR2**. If there is equality for out-degree of each vertex, then an initial vertex should be selected randomly satisfying the second recovery restoration condition (**RR2**). After the obtained vertex $v \in N_D$ observes itself and all of its children (**OR1**), the second phase (PHASE-2) is performed to extend the coverage of unobserved nodes in U by ensuring that **OR2** is applied for each child of $v \in N_D$. For this, from the adjacency matrix $A(G)$ we search the entries a_{ij} of the values of ones in row $v \in N_D$ and apply the following steps:

1) In order, select the first entry (i.e. the child of $v \in N_D$) with a value of one in the current row of $v \in N_D$.
2) Verify that the selected element is not observed yet by checking the set O. If so, then add this element to O and update the set of O and U.
3) After that move on to the row of the selected element (obtained from step 1) and search for the entries having a value of one. In order, select the first entry with a value of one in the current row of this element and apply step 2. If the selected element is already observed, then move back to step 1 and select the next entry of the values of ones in the current row of $v \in N_D$.
4) Keep applying steps 1,2 and 3 till there is no vertex to observe by $v \in N_D$.
5) Now search for the next candidate in N_D and apply the steps 1-4.

Note that if the candidate node $v \in N_D$ is not able to control any more vertex, then it should select the next a vertex having maximum out-degree from the out-degree matrix $D(G)$ and apply PHASE-1 and PHASE-2 repeatedly till we ensure that all the set U are controlled such that the algorithm must be run recursively until $U = \emptyset$.

- **Precondition:** $O = \emptyset$ such that $|N_D - O| \geq 1$.
- **Postcondition:** $U = \emptyset$, and **OR1** and **OR2** are met.
- **Induction:** Assuming that we are in step k ($k > 1$) with $U \neq \emptyset$, $k = |U|$. We apply PHASE-1 and PHASE-2 repeatedly until the candidate node $v \in N_D$ is not able to observe any more vertex, and only after that the set N_D, O, U and k are updated. In the next state $k-1$, the procedure applied is still valid, and therefore, the postcondition $U = \emptyset$ is not fulfilled and PHASE-1 and PHASE-2 must be run again for the next state k until $k = 0$. If $k = 0$, then the remaining unobserved nodes become controlled such that $O = V - N_D$, and therefore the postcondition is met and the algorithm terminates.

V. Experimental Results and Discussions

This section analyses the computational complexity of recovering algorithm; followed by implementation of complete re-computation of N_D for repairing structural controllability on real and model networks including directed Erdős-Rényi networks after N_D has been attacked.

For the computational complexity, the algorithm must find the best candidates N_D, satisfying the two observation rules **OR1** and **OR2**, to ensure the two recovering rules **RR1** and **RR1** are met. For simplicity, we denote $|V| = n$, $|E| = e$, $|N_D| = nd$; the first part of the algorithm is to apply two approaches for recovering the controllability by finding the candidate nd capable of observing the entire U (i.e. it is required to process the entire U where $U = |V|$). **APPR-1** is to find the adjacency matrix of a given network by tracing all its e, where the most time-consuming part of this process is $(O(n+e))$. After the adjacency matrix is obtained, it is necessary to apply **APPR-2** to find the out-degree matrix by searching the entire entries of n in the adjacency matrix in order to obtain the maximum out-degree for each vertex with a cost of $(O(n))$. The overhead of the first part is $O((n+e)+(n)) = O(n^2)$

The second part of the algorithm involves performing the coverage of unobserved nodes in U through PHASE-1 and PHASE-1; the complicated task of these phases is to first find the best driver control candidates that satisfy conditions **RR1** and **RR2**, and these candidates can also provide coverage to each vertex contained in U. To do this, it is required to process the whole entries of the values of ones in each row of N_D in time $O(n-1)$ as it is not allowed to have self-loop in the current entry; for these entries with the values of ones, it must also consider every element containing the values of ones in its rows and check if the coverage of **OR2** can extend with the remaining rows having the values of ones until there is no vertex to cover. In the worst case, if the entire entries of a given matrix have the values of ones except the diagonal entries to avoid self-loop complying with the assumption given III, then the verification of **OR2** can consume time as the execution of algorithm **OR2** continues to check until it reaches the last row of a matrix, where the most time-consuming part for this scenario is $O((n-1)^2.(n-1)) = O(n^3 - 3n^2 + 3n - 1) = O(n^3)$.

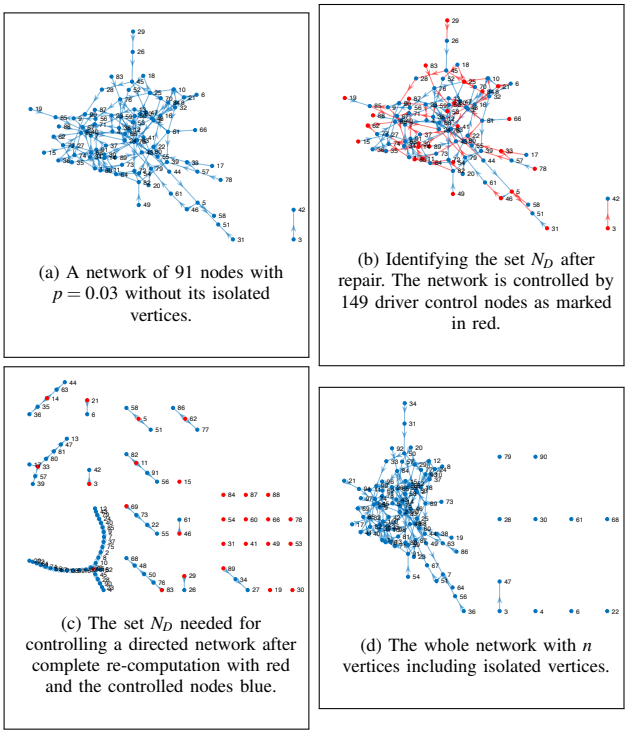
TABLE I. The results of the simulations for different directed ER networks sizes with varying connectivity probabilities.

n	p	e	n_d	$V_{isolated}$
100	0.03	149	27	9
1000	0.0025	1249	296	88
2000	0.0011	2199	602	215
3000	0.0007	3149	919	376

On the other hand, we implemented the strategy and considered connected directed Erdős-Rényi networks with a positive integer n and a probability value $0 \leq p \leq 1$, where n denotes the number of nodes in a network, and p denotes the link probability p such that for all pair of vertices $u, v \in n$, each link (v,u) included in the graph is determined independently with probability p. The development is based on Matlab [1] to produce a more realistic scenario with sparse distributions, using a probability value $0 \leq p \leq 1$ and networks with medium (≤ 1000) and large (≤ 3000) numbers of nodes. The results of the simulations are summarised in Table I, which show the

[1]The code is available from author

efficiency of the recovering strategy with regard to the size of networks when N_D has been perturbed by attacks. Figure 1 shows the restoration process of structural controllability to identify the candidates in N_D for controlling a network of 100 nodes after N_D has been perturbed using the recovering strategy. Note that the isolated nodes are excluded from the network to comply with the assumption given in Section III when performing the algorithm. In addition, the node with in-degree equal to zero must be considered as the candidate in N_D as there is no link pointing out to it as shown in Fig (2b, 2d, 2f). This, however, can increase the number of N_D as the in-degree of links per node can vary as per a connectivity probability value. It can be also deduced from Table I that the variation of the size of the networks can increase the number of driver nodes because the number of links compared to the number of nodes is not high as the connectivity probability value is low. In contrast, by increasing a connectivity probability value of the distribution of links, the number of N_D can become small as shown in Table II and Figure 3. It should be also noted that the instances of N_D are not unique and clearly depend on choosing vertices satisfying **OR1**.



(a) A network of 91 nodes with $p = 0.03$ without its isolated vertices.

(b) Identifying the set N_D after repair. The network is controlled by 149 driver control nodes as marked in red.

(c) The set N_D needed for controlling a directed network after complete re-computation with red and the controlled nodes blue.

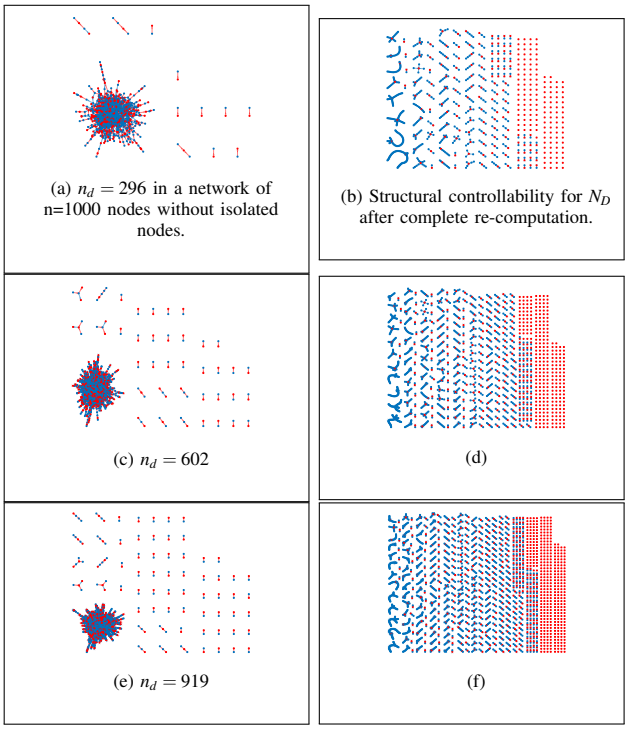
(d) The whole network with n vertices including isolated vertices.

Fig. 1. Recovery of structural controllability for a directed network after N_D has been attacked.

The results confirm also that the recovery of structural controllability can be obtained by searching driver nodes in polynomial time complexity in the worst case n^c, where n is the number of nodes in a given network and c is a constant number. However, the limitation of this strategy requires a trade-off in the complexity against the achievable approximation factor to obtaining optimal driver nodes in a network. This because of the fact that the possibility of effectively checking controllability of a given network is prohibitively expensive for large networks.

TABLE II. THE SIMULATION RESULTS FOR THE CONSTRUCTION OF N_D IN NETWORK SIZE $n = 2000$ NODES WITH VARYING CONNECTIVITY PROBABILITIES.

n	p	e	n_d	$V_{isolated}$
2000	0.0011	2199	611	241
2000	0.0012	2399	594	199
2000	0.0013	2599	566	162
2000	0.0014	2799	560	134



(a) $n_d = 296$ in a network of n=1000 nodes without isolated nodes.

(b) Structural controllability for N_D after complete re-computation.

(c) $n_d = 602$

(d)

(e) $n_d = 919$

(f)

Fig. 2. The complete re-computation of the driver candidates for controlling nodes in different networks sizes as shown in Table I.

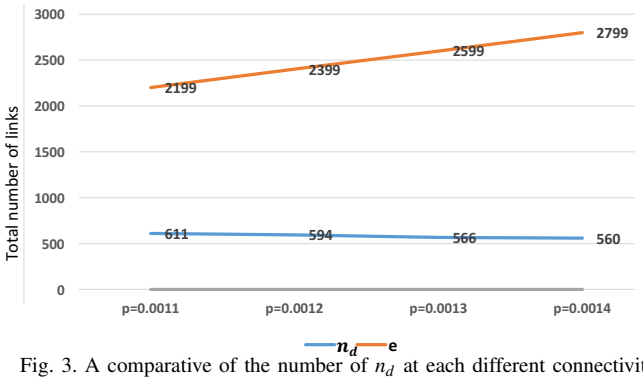


Fig. 3. A comparative of the number of n_d at each different connectivity probabilities with the same network size n=2000.

VI. CONCLUSION

Structural controllability is a highly interesting concept for understanding the properties of critical nodes and its power domination in a control network when a control system is under adverse conditions. The timely recovery of control is

a significant problem in control systems. This requires the ability to recover its damage controllability to ensure high performance and to restore the control network when the driver control nodes have been attacked. The main contribution of this paper is to propose the recovering strategy for controllability in large-scale infrastructure networks using the PDS formulation to understand the effects of topology constraints on the repair strategy. This involves a computationally efficient solution, especially on the Erdős-Rényi networks with directed control links of hundreds of thousands of nodes, by complete re-computing the driver control nodes after an attack. The strategy has been analysed as well as a complexity analysis and the simulation results on model networks provided to show the effectiveness of the recovering strategy. The results highlight that the use of directed Laplacian matrix can be a useful approach for analysing structural controllability of a network. The results highlight also that an increase of a connectivity probability of the distribution of links in ER networks can minimise the number of driver control nodes which is highly desirable while monitoring the entire network as the cost of these devices is rather high. Our future work will further investigate the possibility of maintaining network controllability without complete re-computation if adversaries are able to remove partially implicit links and develop novel methods to improve the restoration of network controllability.

REFERENCES

[1] N. Rashid, J. Wan, G. Quiros, A. Canedo, and M. A. Al Faruque, "Modeling and Simulation of Cyberattacks for Resilient Cyber-Physical Systems", In 13th IEEE Conference on Automation Science and Engineering (CASE), Xi'an, 2017, pp. 988-993.

[2] C.T. Lin, "Structural Controllability", IEEE Transactions on Automatic Control, vol. 19, no. 3, pp. 201-208, 1974.

[3] R.E. Kalman, "Mathematical Description of Linear Dynamical Systems", Journal of the Society of Industrial and Applied Mathematics Contro, Series A1, pp. 152–192, 1963.

[4] Y.Y. Liu, J.J. Slotine, and A.L. Barabási, "Controllability of Complex Networks", Nature 473, pp. 167-173, 2011.

[5] T.W. Haynes, S.M. Hedetniemi, S.T. Hedetniemi, and M.A. Henning, "Domination in Graphs Applied to Electric Power Networks", SIAM Journal on Discrete Mathematics. vol. 15, no. 4, pp. 519-529, 2002.

[6] J. Guo, R. Niedermeier, and D. Raible, "Improved Algorithms and Complexity Results for Power Domination in Graphs. Algorithmica", vol. 52, no. 2, pp. 177-202, 2008.

[7] J. Kneis, D. Mölle, S. Richter, and P. Rossmanith, "Parameterized Power Domination Complexity", Information Processing Letters, vol. 98, no. 4, pp. 145-149, 2006.

[8] U. Feige, "A Threshold of $\ln n$ for Approximating Set Cover", Journal of the ACM, vol. 45, no. 4, pp. 634-652, 1998.

[9] A. Aazami, "Domination in Graphs with Bounded Propagation: Algorithms, Formulations and Hardness Results", Journal of Combinatorial Optimization, vol. 19, no. 4, pp. 429-456, 2012.

[10] C.S. Liao and D.T. Lee, "Power Domination Problem in Graphs", In Proceedings of the 11th Annual International Conference on Computing and Combinatorics (COCOON 2005), 3595, Kunming, China, Springer-Verlag, August 2005, pp. 818-828.

[11] D. Binkele-Raible and H. Fernau, "An Exact Exponential Time Algorithm for POWER DOMINATING SET", Algorithmica, vol. 63, no. 1-2, pp. 323-346, 2012.

[12] A. Aazami and K. Stilp, "Approximation Algorithms and Hardness for Domination with Propagation", SIAM Journal on Discrete Mathematics, vol. 23, no. 3, pp. 1382-1399, 2009.

[13] B. Alwasel and S.D. Wolthusen, "Structural Controllability Analysis via Embedding Power Dominating Set Approximation in Erdős-Rényi Graphs", In the proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications (AINA-2015), Gwangju, Korea, IEEE Press, 2015.

[14] B. Alwasel and S.D. Wolthusen, "Recovering Structural Controllability on Erdős-Rényi Graphs via Partial Control Structure Re-Use", In 9th International Conference on Critical Information Infrastructures Security (CRITIS 2014), Limassol, Cyprus, Springer-Verlag, 2014.

[15] Z. M. Lu and X. F. Li, "Attack Vulnerability of Network Controllability", PloS one, vol. 11, no. 9, 2016.

[16] C.L. Pu, W.J. Pei, and A. Michaelson, "Robustness Analysis of Network Controllability", Physica A: Statistical Mechanics and its Applications, vol. 391, no. 18, pp. 4420-4425, 2012.

[17] P. Holme, B.J. Kim, C.N. Yoon, and S.K. Han, "Attack Vulnerability of Complex Networks, Physical Review E, vol. 65, no, 5, 2002.

[18] B. Alwasel and S.D. Wolthusen, "Recovering Structural Controllability on Erdős-Rényi Graphs in the Presence of Compromised Nodes", In 10th International Conference on Critical Information Infrastructures Security (CRITIS 2015), Berlin, Germany, Springer-Verlag, 2015.

[19] C. Alcaraz and S.D. Wolthusen, "Recovery of structural controllability for control systems, In Jonathan Butts and Sujeet Shenoi, editors, Critical Infrastructure Protection VIII, Berlin, Heidelberg, Springer, 2014, pp. 47-63.

[20] C. Alcaraz, E. E. Miciolino, and S.D. Wolthusen, "Structural Controllability of Networks for Non-interactive Adversarial Vertex Removal", In Proceedings of the 8th International Workshop on Critical Information Infrastructures Security (CRITIS 2013), 8328, Amsterdam, The Netherlands, Springer-Verlag, 2013, pp. 120-132.

[21] M. Barthélemy, "Betweenness Centrality in Large Complex Networks", The European Physical Journal B: Condensed Matter and Complex Systems, vol. 38, no. 2, pp. 163-168, 2004.

[22] Y.Y. Liu, J.J. Slotine, and A.L. Barabaśi,, "Control Centrality and Hierarchical Structure in Complex Networks", Public Library of Science ONE, vol. 7, no. 9, pp. 1-7, 2012.

[23] S. Zhang and S. D. Wolthusen, "Efficient Control Recovery for Resilient Control Systems,"In 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, IEEE, 2018, pp. 1-6.

[24] S. Zhang and S. D. Wolthusen, "Efficient Analysis to Protect Control into Critical Infrastructures", In International Conference on Critical Information Infrastructures Security, Cham, Springer, 2018, pp. 226-229.