Robustness Analysis Of Structural Controllability for Directed Networks Against Single Edge Attacks

Bader Alwasel

***Abstract**: Infrastructure systems are an essential component, evolving with greater interconnectivity and interdependence at varying degrees. The control robustness of a network against malicious attack and random failure also becomes a further considerable problem in network controllability and its robustness. An adversary who is adequately knowledgeable about the control system can take control of aspects of the network as it can compromise the control network's subset of critical nodes and/or disconnect parts of the control network resulting in low observability. Therefore, safeguarding critical infrastructure systems from different disruptions is primarily significant. This paper focuses the POWER DOMINATING SET (PDS) problem, originally introduced by Haynes to study the structure of electric power network control systems and their efficient control, as an alternate framework for the examination of the structural controllability of networks. However, PDS is generally known to be NP-complete with low approximability with recent work focusing on studying properties of restricted graph classes. Based on the PDS problem, this paper also is dedicated to studying the different edge attack strategies, as well as the robustness of network controllability of Erdo˝s-Re´nyi networks with directed control links under single edge attacks. MATLAB will be utilised in order to produce a simulative evaluation for more realistic critical infrastructure networks such as real power networks.*

***Keywords**: Complex Network; Structural Controllability; Attack Models; Cyber Physical Systems*

I. INTRODUCTION

Securing control systems have received much attention to many researchers from various areas [1]. Robustness is defined as the capacity to tolerate disturbances and faults, and it is an essential feature of complex systems and networks [2]. One issue which is particularly significant, in relation to the operation of a complex network, is the robustness of the entire system in safeguarding against the failure of any integral components [3]. Accordingly, the robustness of network structural controllability is the capability to maintain structural control over the rest of the network following malicious attacks or random failures. This issue has been broadly studied, in particular following the examination put forward by Lin [4] on structural controllability. One of Lin's key contributions was to give a graph-theoretical interpretation to Kalman algebraic criterion [5]. This enables the identification of essential and adequate conditions, in order to determine individual driver nodes which are capable of controlling a system, within a predefined structure (topology). Informally, controllability requires that a desired configuration can be forced from an arbitrary configuration in a finite number of steps. By control theory [5], a Linear Time-Invariant (LTI) system is represented by a state equation:

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

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

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

Whilst Kaman's rank criterion is only achievable for small networks, the computation of rank for larger networks, like power networks or considerable control systems, for example, is exceedingly costly. This because of the fact that there are computational complexities involving identifying all potential combinations which in the worst-case scenario necessitates 2^n-1 different combinations. To avoid this problem and still design or analyse controllable LTI systems, Lin [4] 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, $V_\mathbf{B}$ consists of nodes able to inject control signals into the whole network, also known as driver nodes (N_D) corresponding to input vector u in Equation (1). In control systems, the ability to identify driver nodes must be considered crucial for both attackers and defenders in control systems. Liu *et al*. [6] established that a minimum number of driver node subsets can be found out in the Maximum Matching approach. This paper, however, considers the alternative approach originally suggested by Haynes *et al*. [7], in order to study electric power networks and the expansion of the well-known Dominating Set (DS) problem, in relation to the PDS problem. An alternative formulation can be acquired by way of the PDS approach, which enables the identification of the minimum N_D.

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author

Bader Alwasel*, Department of Applied Natural Sciences, Computer Science, Unaizah Community College, Qassim University, Saudi Arabia. Email: bwasel@qu.edu.sa

The removal of power links, however, whether by accidental failure or planned attacks, can result in a worldwide redistribution of burdens across the whole network.
This redistribution may increase the load, on some nodes, and links to the extent that they surpass their capabilities, prompting an increasing number of excess failures. The contribution of this paper is, therefore, to expand further the attack scenarios from [8] to varying edge attack strategies on structural controllability of directed Erdős-Rényi networks. Then we analyse the robustness of network controllability of directed Erdős-Rényi networks under non-interactive single edge attacks (i.e. where it is presumed that attackers select a single-edge attack model at a time). This practical interest in network control is primarily based in the real-world context, due to the considerable parallels existing between the logical structures of PDS-based networks and the remote monitoring real-world systems, where driver nodes are illustrated by PDS in electrical power network control (i.e. control terminal units which control industrial sensors or actuator networks).

The remainder of the paper is structured as follows. Section **II** reviews the related work and network controllability considering vulnerability. Section **III** describes the network model as well as different edge attack strategies on structural controllability. We then proceed to evaluate the impact of such attacks on the network controllability and observability in Section **IV** discussing the simulation results and close this paper with some conclusions and our on-going work in Section **V**.

II. POWER DOMINATION AND CONTROLLABILITY OF NETWORKS

Domination, an important concept of graph theory, can be viewed as a substantial aspect of control systems' design and analysis, as it is comparable to the controllability problem described by Kalman. Haynes *et al*. [7] investigated theoretical properties of the PDS problem in terms of the graph-theoretical representation as a framework for studying electric power systems and their effective monitoring. One apparent concern of edge removal from a minimal power dominating set is the reconstruction and recovery of control. The authors of [7] have demonstrated that the PDS for a particular graph G is **NP**-complete with reference to general graphs, albeit being limited to particular classes of graphs, namely chordal graphs and bipartite graphs. They further put forward a linear time algorithm in relation to the PDS problem in trees. The PDS problem has also been determined to be **NP**-complete in consideration of planar graphs, circle graphs, and split graphs, as well as that the fact there is no better way to approximate than through the domination problem for general graphs [9]. Moreover parameterised results have been put forward [9],[10], confirming W[2]-hardness in the event where the parameter's size corresponds to that of the resolution, by way of decreasing a DS to a PDS. Moreover, Guo *et al*. [9] demonstrated the fixed-parameter tractability of PDS in relation to a tree decomposition, of bounded-tree width, for the underlying graph, while simultaneously introducing a concrete algorithm which can develop PDS into an orientation problem in undirected graphs. As the PDS problem is a generalisation of the Dominating Set (DS) problem, the basic minimum DS problem is **NP**-complete using a polynomial-time approximation factor of $\theta(\log n)$ as shown by Feige [11]. Therefore, Aazami and Stilp [12] made a distinction between the approximation hardness of DS and PDS problems and confirmed that, unless $\mathbf{NP} \subseteq DTIME(n^{polylog(n)})$, it is unlikely that a better result other than using $2^{\log^{1-\epsilon} n}$ to approximate the PDS problem, can be achieved. They further suggested an $O(\sqrt{n})$-approximation algorithm for the PDS problem in planar graphs. Another **NP**-completeness proof for the PDS problem in split graphs has been presented by Liao and Lee [13], as well as a polynomial-time algorithm for optimally solving PDS on interval graphs. Binkele-Raible and Fernau further demonstrate that the PDS problem persists as **NP**-hard on cubic graphs [14], and Guo *et al*. show valid orientations designed to optimally resolve PDS on undirected graphs with bounded-tree width. Furthermore, the Directed PDS (DPDS) was redefined by Aazami and Stilp [15] as valid colourings of edges, and they established a dynamic programming algorithm involving a DPDS, where the underlying undirected graph possessed a bounded-tree width. The previous work has been conducted to investigate literature on graph classes, in which PDS has been reviewed [16]. Also, it determined that such structures could be integrated into Erdős-Rényi graphs having varied density and approximation characteristics, which could be utilised in applying the concepts to resolve the PDS problem. An algorithm has been designed in order to reduce an average-case complexity in relation to (directed) control graphs through the use of the remaining fragments of the original graph, where possible [17]. This helped to identify edges which were not formerly utilised for reducing the number of PDS.

The authors of [18] studied the nodes and edges attack vulnerability of network controllability for the canonical model networks according to five different strategies. Wang *et al*. [19] analysed the robustness of controllability of various random graph classes, inclusive of the degree sequences discovered in current (i.e. complex) networks. They examined the way in which it is possible to sustain structural controllability when malicious attacks take place on directed networks and combined the control robustness problem with the transitivity maximisation problem for control routes. Furthermore, Pu *et al*. [2] have identified the impact of random and targeted vertex removal concerning matchings in Erdős-Rényi random graphs and scale-free graphs; notwithstanding that latent consequences have already been meticulously established by Bollobas and Riordan [20]. It is further essential to observe the findings of Sudakov and Vu [21] on graph resilience, in relation to both local and global properties. The authors of [22] proposed an algorithm to repair the structural controllability of the residual network without re-computing a maximum matching of digraph. An efficient algorithm to identify vulnerable single vertices to malicious removals and failures is designed by [23]. It should be noted that it is possible to attack edges, in which the attacks on vertices can be in the form of servers breaking down because of malicious attackers, and hence, edges' attack involves communication cables getting disconnected.

Nie *et al*. [24] also carried out a significant study considering the controllability of the directed Erdo˝s- Re´nyi and examined the robustness of the controllability of Erdo˝s-Re´nyi networks as per different parts of the cascading failures, created by removing only the highest load edge (i.e. the load on edge e_{ij} is the total number of shortest paths in network passing through the e_{ij} at time t). They observed that networks' controllability changes as cascading failures take place when there are two specific attack strategies, which are intentional and random. Moreover, the author of [25] evaluated the vulnerability of various complex networks including the undirected Erdo˝s-Re´nyi model of random networks regarding diverse edge attacks. A study by [26] also assessed adding edge directions, as per the node residual degree, to enhance complex network controllability and presented a technique to develop edge direction for presenting the proposed method's effectiveness regarding the two basic network models Erdo˝s-Re´nyi and scale-free networks. The classification of all edges of a minimum-input structurally controllable in digraphs into critical, redundant and ordinary categories was studied by [27]. This allows to determine vulnerable edges to the removal and effectively repair network structural controllability.

III. NETWORK AND ATTACK SCENARIOS ON STRUCTURAL CONTROLLABILITY

A. Network Model

In this paper, we consider unweighted directed graph *G(V,E)* with an arbitrary set of nodes *V* and a set of edges *E*, generated by Erdo ˝s-Re´nyi random graph class *ER(n,p)* [28]. Each directed edge included in the graph is determined independently with probability *p*. As a result, we consider only the resulting instance of *ER(n,p)* that is a connected acyclic graph without its isolated vertices such that the resulting graph has no multi-edges, but may have two edges with different directions on the same ordered pair of vertices (called anti- parallel edges). This paper focuses on the problem of structural controllability for determining a minimum set of driver nodes in directed networks. To do this, we follow the approach based on the PDS problem, which is an equivalent formulation for identifying minimum driver node subsets [7]. These driver nodes belonging to V can be obtained from the two observation rules for controllability, simplified by Kneis *et al*. [10] from the original formulation by Haynes, *et al*. [7]:

[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 $d\text{-}1$ observed vertices, then the remaining unobserved neighbour becomes observed as well.

The construction of N_D is relied on choosing nodes that fulfil **OR1** and such N_D control all vertices in $V \setminus N_D$ through utilising **OR2**. To identify a PDS (or set of N_D) for a given graph complying with the assumption above, we follow the re-covering strategy defined in [29] to complete re-computation of the N_D structure; this algorithm is based on the use of directed Laplacian matrix for analysing structural controllability of a network. Note that the instances of a PDS (or set of N_D) are not unique and subjected to the selection of vertices satisfying **OR1**.

B. Threat Model

To evaluate the robustness of controllability of directed Erdo˝s-Re´nyi networks in terms of the network connectivity and observability (as the dual of controllability), we investigate the different edges attack patterns that may result in the breakdown of the network into pieces and destroy the control network in order to leave parts of a system unobserved or isolated by N_D. Throughout our study, we do not consider methods of responses of defenders against the attacks presented here. However, we assume that edges are removed from nodes in N_D or dependent nodes by one or multiple attackers with prior knowledge about the whole network structure, its structural control, or its power domination relation, and the identities of the current minimum set of driver nodes N_D. These threats are based on non-interactive single edge attacks in which an adversary at each time step can attack a selected removal of power links according to the type of the attack scenario described below. Note that in realistic scenarios, these malicious threats can be exploited by either internal users who have legitimate access to the network such as human operators or external attackers who may know the vulnerabilities of the deployed networks or learn from the network topology to bypass security controls and penetrate the entire network or parts of the control network. We then analyse the behaviour of the control network after an attack according to five attack scenarios (denoted here as **AS*i***) described below:

AS$_1$ An attacker could randomly delete all edges from a vertex in N_D with the highest out-degree.

AS$_2$ Randomly remove some (but not all) edges from a vertex within N_D with the highest out-degree.

AS$_3$ Randomly delete some (but not all) edges from a vertex in N_D with the minimum out-degree.

AS$_4$ Randomly remove an edge from a vertex not belong to N_D (i.e. remove one edge in the middle of a directed control path).

AS$_5$ Randomly delete an edge from last element v of dependent nodes in the ordered set obtained by N_D.

IV. SIMULATION RESULTS AND DISCUSSIONS

This section tests the robustness of controllability of directed Erdo ˝s-Re´nyi networks at different attack patterns, as triggered by the removal of edges, through Matlab simulations[1]. The evaluation of the control robustness of a directed network is only considered when an adversary capable of independently exploiting five attack scenarios in a single- round of attacks. For each attack scenario we assume that a single edge or several edges can be targeted by an attacker as described in subsection III-B. We then investigate the robustness of network controllability of directed

[1] The code is available from author

Erdo˝s-Re´nyi networks under the adversarial scenario of single edge attacks by calculating:

1) the number of targeted edges per an attack scenario,
2) the size of driver nodes needed for controlling a network after each attack scenario.
3) the observation rate (the remaining observable nodes after attack as a percentage (**OR1**), and
4) the number of affected nodes after an attack scenario.

As most of the large real network is sparse, we generate connected directed Erdo˝s-Re´nyi networks with n nodes where any ordered pair of nodes $u,v \in n$ is connected by a directed link with probability p. In the experimental simulation, we model networks with small (≤ 100) and large (≤ 4000) numbers of nodes using a probability value $0 \leq p \leq 1$ to produce more realistic critical infrastructure networks such as real power networks. Building on previous work [29], the results of complete re-computation of a PDS (or set of N_D) for controlling nodes in different networks sizes are shown in Table I. This approach is based on the recovering strategy for re-computation N_D using the PDS formulation, which is described in more detail in [29].

TABLE I: The computational simulation results for identifying the minimum number of a PDS (or set of N_D) in different directed ER networks sizes with several connectivity probabilities.

Nodes	p	Edges	n_d	$V_{isolated}$
100	0.04	198	26	2
500	0.0056	699	147	31
1000	0.0024	1199	294	98
2000	0.0011	2199	616	212
3000	0.00071	3194	920	365
4000	0.00051	4079	1206	516

After executing five threat models shown in subsection III-B, we obtain from Figure 1 that $\mathbf{AS_1}$ is harm to the network controllability, where it is prone to the cascading edge failure caused by removing a single driver node of maximum out-degree. This is predicted as n_d controls the highest number of observed nodes and this may become targets of attackers to disrupt controllability of dependent nodes into non-controllable parts and damage the current control network. As a result, the number of n_d needed for controlling the attacked network significantly increases when the network is subjected to this attack scenario as shown in Figure 2. This is because the disjoint dependency paths have been disconnected from n_d of the largest out-degree by the removal of all its links. This means that the number of connected components, that are disconnected from the whole network, may increase by the number of the edges removal from a single driver node of the maximum out-degree. Also, the results in Figure 1 show that cascade failures can also be more harmful to network controllability even if they are triggered by the removal of some but (not all) edges of a single driver node of maximum out-degree as described by $\mathbf{AS_2}$. Besides, the harmfulness caused by attacking an edge from a node not belong to N_D has less effect on the controllability of dependent nodes as confirmed in Figure 1. The reason for this lies in the fact that the nature of $\mathbf{AS_4}$ and $\mathbf{AS_5}$ targets only the critical nodes with out-degree equal to one. Therefore, the fraction of n_d needed for controlling the compromised networks is small enough which means the control network is more robust to cascading failures caused by $\mathbf{AS_4}$ and $\mathbf{AS_5}$, as illustrated in Figure 2.

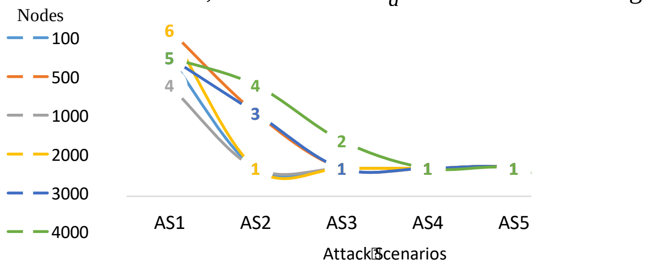


Fig. 1: The fraction of edges removal for each scenario at a single-round of non-interactive edge attacks.

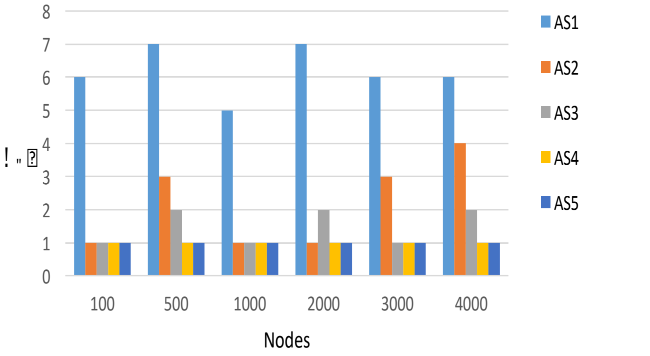


Fig. 2: No. of n_d needed for controlling the network after an attack scenario AS_i.

Compared with $\mathbf{AS_4}$ and $\mathbf{AS_5}$, the results indicate that there is a small variation in the number of n_d required to take over control the compromised parts when executing $\mathbf{AS_3}$.

For observability, Table II shows that each network lost its controllability of dependent nodes, and therefore, a significant reduction in its observability would be affected as a result. This reduction is even more notable when $\mathbf{AS_1}$, $\mathbf{AS_2}$ and $\mathbf{AS_4}$ are independently executed but lost of observability is not obvious when the network controllability is targeted by $\mathbf{AS_5}$. This means that lost observability is not only dependent on exploiting driver nodes as described by $\mathbf{AS_1}$, $\mathbf{AS_2}$ and $\mathbf{AS_3}$, but also on the critical dependent nodes that do not belong to N_D as described in $\mathbf{AS_4}$. The results also show that there is no significant impact on the observability rate when a network is targeted by $\mathbf{AS_3}$ in the comparison with $\mathbf{AS_1}$, $\mathbf{AS_2}$ and $\mathbf{AS_3}$. However, this can not be taken as a measure for the influence of this attack scenario on network controllability, where the mechanism of $\mathbf{AS_3}$ randomly deletes only some (but not all) links from a node in N_D with the minimum out-degree. Therefore, the disjoint dependency paths that are disconnected from n_d of the minimum out-degree after an attack may become at most one dependency path in the best case.

TABLE II: Observation rate after each attack scenario.

	100	500	1000	2000	3000	4000
AS$_1$	58.16	91.68	95.56	95.63	99.24	99.56
AS$_2$	98.97	98.08	99.77	99.83	99.46	99.77
AS$_3$	96.93	99.57	99.66	99.88	99.96	99.82
AS$_4$	96.93	97.86	99.55	99.83	99.84	99.85
AS$_5$	98.97	99.79	99.88	99.94	99.96	99.97

A considerable fraction of vulnerable nodes per an attack scenario is shown in Table III, where the results confirm that the number of compromised nodes can increase when more power links are being attacked. As a result, when attackers seek to disrupt the power domination relation by removals of power links, the number of N_D required to control compromised parts may become much more. This requires a trade-off between the robustness of network structural controllability against edge removals and lower control cost with a minimal power dominating set. The simulation results from Table II and Table III highlight that the network size with less than 500 nodes would be affected heavily during the attack, while for networks with more nodes, they remain broadly stable. It should be noted that most of the observation rates maintain high (above 91% of observability) after attack, that is because we only simulate a single-round of edge attacks on networks in order to understand the behaviour of network controllability under vulnerability for networks of non-interactive single edge attacks. However, the networks would largely lose observability if they are targeted by the removal of edges in multiple-round attacks in the worst case.

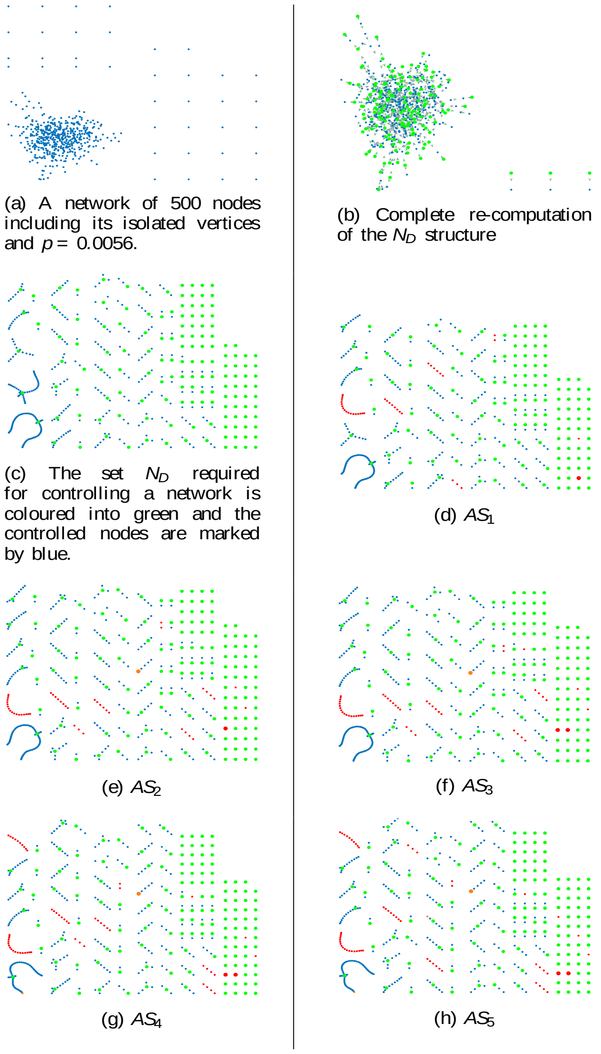
TABLE III: The number of vulnerable nodes per an attack scenario.

	100	500	1000	2000	3000	4000
AS$_1$	41	39	40	78	20	15
AS$_2$	1	9	2	3	14	8
AS$_3$	3	2	3	2	1	6
AS$_4$	3	10	4	3	4	5
AS$_5$	1	1	1	1	1	1

Figures 3 illustrates the threat model based on five edge attack scenarios (**AS$_i$**) for a directed network of 500 nodes, generated according to Erdo˝s-Re´nyi model, shown in Table I through Matlab simulations. Note that each Sub-figures 3d, 3e, 3f, 3g and 3h shows the evolutions of all the adversarial attacks that occurred in the previous scenarios including the current threat model. The experimental simulations of adversarial attacks for the most networks shown in Table I are presented in the Appendix.

V. CONCLUSION

In this paper we have analysed the robustness of network structural controllability through the POWER DOMINATING SET problem. We have also tested the robustness of controllability of random Erdo˝s-Re´nyi, with an emphasis on directed networks with different connectivity probability, under a single-round of several non-interactive single-edge attack types. We reported that the edge attack strategy of type **AS$_1$** has more effects on network robustness and structural properties of network controllability compared to the other attack scenarios, and this is obvious when a single driver node of maximum out-degree is vulnerable to attacks. Therefore, the number of driver nodes required for controlling the network continuously increases along with an increase of arbitrary removal of edges on the original total amount when the network subject to this type of threat scenarios. As a result, it may affect control cost to repair network structural controllability with a minimum set of driver nodes. In contrast, the networks are very robust to attacks of type **AS$_5$** which means the damage of this threat to network observability is not very significant. Our future works aim to extend this analysis when a network is vulnerable to multiple-round of five combined attack models presented here. Also, we endeavour to enhance the robustness of network structural controllability to maintaining domination properties when adversaries are able to remove partially power links.


(a) A network of 500 nodes including its isolated vertices and $p = 0.0056$.

(b) Complete re-computation of the N_D structure

(c) The set N_D required for controlling a network is coloured into green and the controlled nodes are marked by blue.

(d) AS_1

(e) AS_2

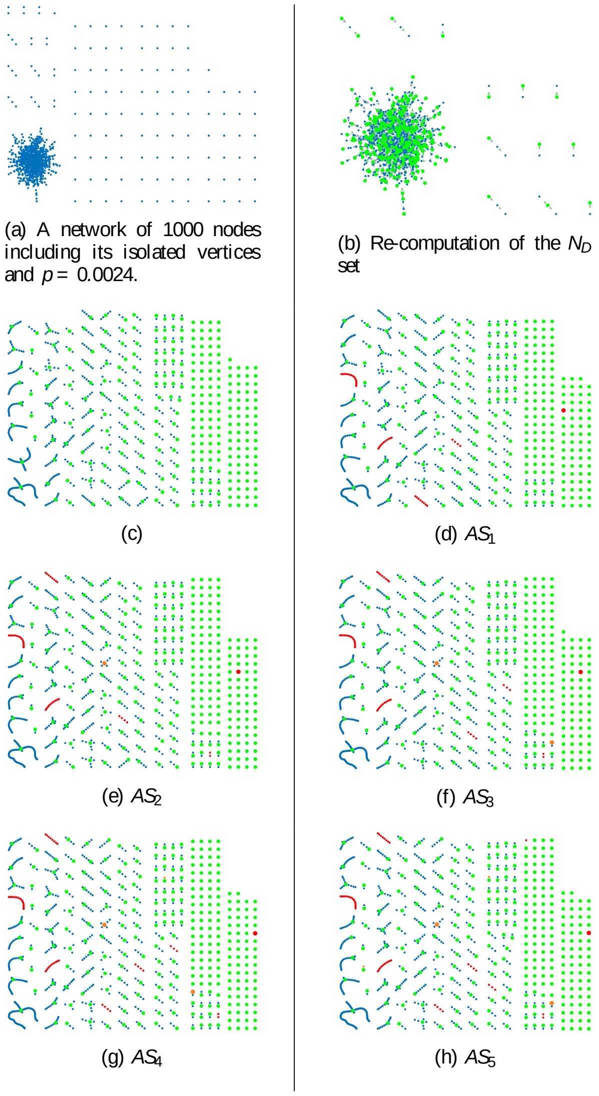
(f) AS_3

(g) AS_4

(h) AS_5

Fig. 3: Various attack strategies (AS_i) for a single-round of non-interactive edge attacks applied to connected a directed network of 500 nodes. Nodes with red colour denote the unobserved nodes that are completely isolated from a given network after links removal attacks, and vulnerable vertices with a selected removal of links are denoted by orange colour.

APPENDIX



(a) A network of 1000 nodes including its isolated vertices and $p =$ 0.0024.

(b) Re-computation of the N_D set

(c)

(d) AS_1

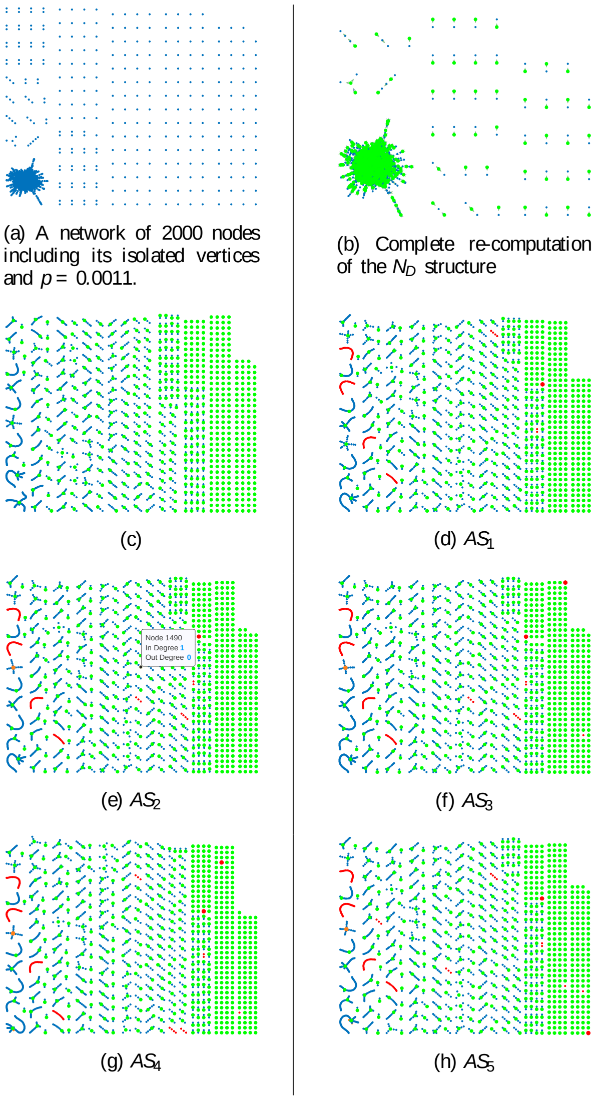
(e) AS_2

(f) AS_3

(g) AS_4

(h) AS_5

Fig. 4: A directed network of 1000 nodes is prone to five different strategies (AS_i).



(a) A network of 2000 nodes including its isolated vertices and $p =$ 0.0011.

(b) Complete re-computation of the N_D structure

(c)

(d) AS_1

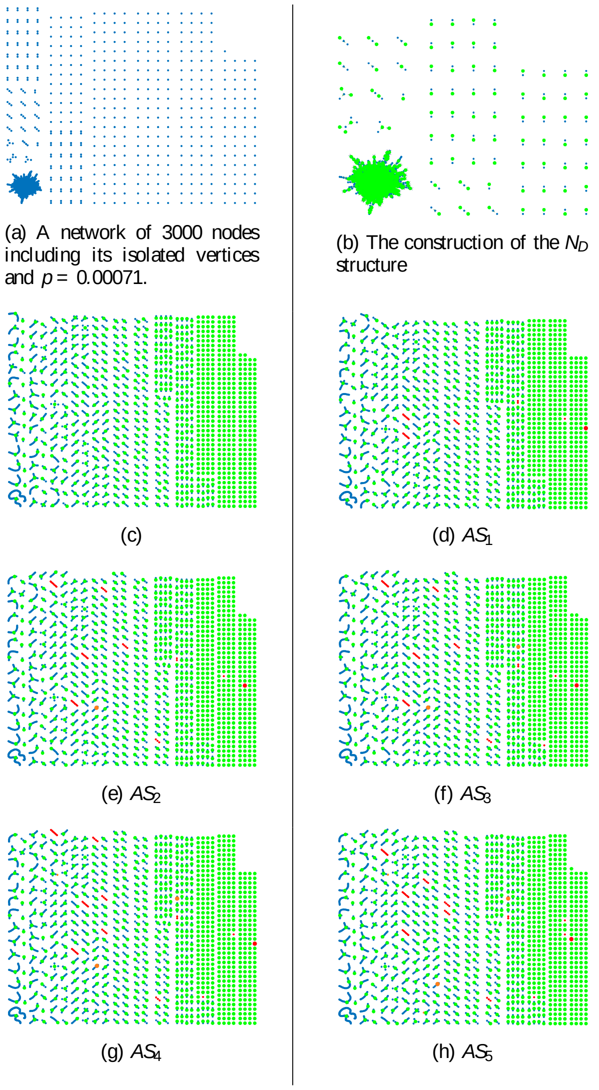
(e) AS_2

(f) AS_3

(g) AS_4

(h) AS_5

Fig. 5: The evolutions of all the adversarial attacks (AS_i) applied to a directed network of 2000 nodes.



(a) A network of 3000 nodes including its isolated vertices and $p = 0.00071$.

(b) The construction of the N_D structure

(c)

(d) AS_1

(e) AS_2

(f) AS_3

(g) AS_4

(h) AS_5

Fig. 6: Various attack strategies (AS_i) for a single-round of non-interactive edge attacks applied to a connected directed network of 3000 nodes.

REFERENCES

1. Rashid, N., Wan, J., Quiros, G., Canedo, A., and Al Faruque, M. A. "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. Pu, C.L., Pei, W.J., Michaelson, A. "Robustness Analysis of Network Controllability", Physica A: Statistical Mechanics and its Applications, vol. 391, no. 18, pp. 4420-4425, 2012.
3. Albert, R., Jeong, H., and Baraba´si, A.-L. "Error and attack tolerance of complex networks", Nature vol. 406, 6794, pp. 378382, 2000.
4. Lin, C.T., "Structural Controllability", IEEE Transactions on Automatic Control, vol. 19, no. 3, pp. 201-208, 1974.
5. Kalman, R.E. "Mathematical Description of Linear Dynamical Systems", Journal of the Society of Industrial and Applied Mathematics Contro, Series A1, pp. 152192, 1963.
6. Liu, Y.Y., Slotine, J.J., Baraba´si, A.L. "Controllability of Complex Networks", Nature 473, pp. 167-173, 2011.
7. Haynes, T.W., Hedetniemi, S.M., Hedetniemi, S.T., Henning, M.A., "Domination in Graphs Applied to Electric Power Networks", SIAM Journal on Discrete Mathematics. vol. 15, no. 4, pp. 519-529, 2002.
8. Alcaraz, C., Miciolino, E. E., and Wolthusen, S. D. "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.
9. Guo, J., Niedermeier, R., Raible, D. "Improved Algorithms and Complexity Results for Power Domination in Graphs. Algorithmica", vol. 52, no. 2, pp. 177-202, 2008.
10. Kneis, J., Mo¨lle, D., Richter, S., Rossmanith, P. "Parameterized Power Domination Complexity", Information Processing Letters, vol. 98, no. 4, pp. 145-149, 2006.
11. Feige, U. "A Threshold of ln n for Approximating Set Cover", Journal of the ACM, vol. 45, no. 4, pp. 634-652, 1998.
12. Aazami, A. "Domination in Graphs with Bounded Propagation: Algorithms, Formulations and Hardness Results", Journal of Combinatorial Optimization, vol. 19, no. 4, pp. 429-456, 2012.
13. Liao, C.S., Lee, D.T. "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.
14. Binkele-Raible, D., Fernau, H. "An Exact Exponential Time Algorithm for POWER DOMINATING SET", Algorithmica, vol. 63, no. 1-2, pp. 323-346, 2012.
15. Aazami, A. and Stilp, K. "Approximation Algorithms and Hardness for Domination with Propagation", SIAM Journal on Discrete Mathematics, vol. 23, no. 3, pp. 1382-1399, 2009.
16. Alwasel, B. and Wolthusen, S. D. "Structural Controllability Analysis via Embedding Power Dominating Set Approximation in Erdo˝s- Re´nyi Graphs", In the proceedings of the 29th IEEE International Conference on Advanced Information Networking and Applications (AINA- 2015), Gwangju, Korea, IEEE Press, 2015.
17. Alwasel, B. and Wolthusen, S. D. "Recovering Structural Controllability on Erdo˝s-Re´nyi Graphs via Partial Control Structure Re-Use", In 9th International Conference on Critical Information Infrastructures Security (CRITIS 2014), Limassol, Cyprus, Springer-Verlag, 2014.
18. Lu, Z. M and Li, X. F. "Attack Vulnerability of Network Controllability", PloS one, vol. 11, no. 9, 2016.
19. Wang, B., Gao, L., Gao, Y., & Deng, Y. "Maintain the Structural Controllability under Malicious Attacks on Directed Networks", Europhysics Letters, vol. 101, no. 5, 2013, pp. 1-6.
20. Bollobs, B and Riordan, O. "Robustness and Vulnerability of Scale-Free Random Graphs", Internet Mathematics, vol. 1, no. 1, 2003, pp. 1-35.
21. Sudakov, B. and Vu, V. H. "Local Resilience of Graphs. Random Structures and Algorithms", vol. 33, no. 4, 2008, pp. 409-433.
22. Zhang, S. and Wolthusen, S. D. "Efficient Control Recovery for Resilient Control Systems", In 15th International Conference on Networking, Sensing and Control (ICNSC), Zhuhai, IEEE, 2018, pp. 1-6.
23. Zhang, S. and Wolthusen, S. D. "Efficient Analysis to Protect Control into Critical Infrastructures", In International Conference on Critical Information Infrastructures Security, Cham, Springer, 2018, pp. 226-229.
24. Nie, S., Wang, X., Zhang, H., Li, Q., and Wang, B. "Robustness of Controllability for Networks Based on Edge-Attack", Public Library of Science ONE, vol. 9, no. 2, 2014, pp. 1-8.
25. Holme, P., Kim, B. J., Yoon, C. N., and Han, S. K. "Attack Vulnerability of Complex Networks", Physical Review E, vol. 65, no, 5, 2002.
26. Lv-Lin, H., Song-Yang, L., Gang, L., and Liang, B. "Controllability and Directionality in Complex Networks", Chinese Physics Letters, vol. 29, no. 10, 2012.
27. Zhang, S. and Wolthusen, S. D. "Security-aware network analysis for network controllability", In 32nd International Conference on Advanced Information Networking and Applications Workshops (WAINA), IEEE, 2018.
28. Bollobs, B. "Random Graphs", volume 73 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, UK, 2nd edition, 2001.
29. Alwasel, B. "Recovery of Structural Controllability into Critical Infrastructures under Malicious Attacks", International Journal of Advanced Computer Science and Applications, vol. 11, no. 4, 2020, pp. 723-728

AUTHOR PROFILE

Bader Alwasel is currently an Assistant Professor at Qassim University. His main research interests include Cyber-Physical Systems Security, Network & Distributed Systems Security, Control Systems, Graph Theory, and Models for Critical Infrastructure Protection.