Chapter 1

Introduction

This chapter provides an overview of network controllability and controllability robustness, presenting the development from classical control theory to modern network science. It reviews some foundational concepts, including structural and exact controllability, highlights recent advances addressing conventional, temporal and multilayer networks, and discusses energy-efficient and targeted control strategies. It examines the growing importance of robustness against random failures and hostile attacks, and formulates key research questions on maintaining functionality and optimizing robustness. It outlines the emerging machine learning techniques for analyzing dynamics, evaluating robustness, and optimizing structures. The chapter concludes with the motivation and organization of the book, positioning controllability robustness as a critical challenge for secure and resilient networked systems in dynamic and adversarial environments.

The chapter is organized as follows. Section 1.1 presents a brief overview of network controllability and controllability robustness. Section 1.2 discusses practical applications of the subjects across diverse domains. Section 1.3 examines various risks posed by adversarial attacks and their implications for network controllability robustness. Section 1.4 provides the motivation and outlines the structure of the book.

1.1 Overview of Network Controllability and Controllability Robustness

Controllability is a fundamental concept in control theory and network science, indicating the ability to steer a networked system from an initial state to a target state by a limited external input, called control, in finite time.

In this book, only networks of linear or linearized dynamical systems are studied. Recently, research on such linear network controllability has attracted substantial attention because of the significance and applicability of this concept across diverse domains, including biological networks such as gene regulatory and metabolic pathways, neural networks underlying cognitive processes, epidemiological networks modeling disease transmission, social networks governing information diffusion and influence propagation, engineered infrastructures such as power grids and transportation systems, logistical networks ensuring supply chain robustness, financial networks managing systemic risks, and communication networks supporting large-scale data transmission and distributed computing [1–5].

Verifying the controllability of a linear or linearized dynamical network is vital in engineering and technology, which ensures that a system in concern can meet theoretical and practical requirements for designated control tasks as well as reliability under varying conditions. Common methods include the Kalman rank condition [1, 6–8], the Popov-Belevitch-Hautus (PBH) rank condition [9], and the graph-theoretic criterion for structural controllability [10]. Simulation-based and energy-based approaches [11] are also useful for evaluating network controllability under realistic constraints, considering essential issues such as network structures, control nodes, and component dynamics.

The origins of network controllability can be traced back to the classical control theory on linear dynamical systems, particularly the foundational work of Kalman in the 1960s [1, 6, 8]. Kalman introduced the concept of controllability and established a criterion based on a system matrix, called the controllability matrix, which provides a rigorous mathematical framework for determining whether a linear system can be fully controlled by bounded external inputs in finite time. This principle was later extended to interconnected linear dynamical systems, forming a basis for the network control theory applicable to complex dynamical networks.

The classical notion of controllability in control theory primarily addresses the intrinsic dynamics of a single higher-dimensional linear system. With the emergence of network science in the early 2000s, one research focus was the extension of the system controllability toward the controllability of large-scale complex networks [12–14]. In such networks, nodes represent dynamical subsystems and edges capture the interactions among them, encompassing scientific, engineering and technological domains such as the Internet, power grids, transportation systems, neural networks, social networks and financial networks [4].

In the era of pervasive connectivity, Liu, Slotine, and Barabási advanced the classical concept of structural controllability [10], establishing a fundamental link between directed network topology and system controllability by introducing a driver node algorithm based on the maximum matching principle from graph theory, which identify the minimal set of nodes required to achieve full control of the network.

Building on this notion, the framework of exact controllability emerged as a complementary approach to refine the understanding of network controllability [9]. It determines the network controllability by considering both network topology and precise numerical values of system parameters. Diferring from the structural controllability, which depends solely on the zero or nonzero structure of the network controllability matrix and holds for almost all parameter choices, exact controllability provides a parameter-specific analysis. The minimal number of driver nodes required for full control of the network is equal to the maximum geometric multiplicity of the eigenvalues of the system controllability matrix, or the maximum algebraic multiplicity for diagonalizable undirected networks. Driver node locations are identified using the PBH rank condition with appropriate elementary matrix transformations. This approach applies to networks with arbitrary structures and edge weights and provides a universal tool for assessing controllability of directed or undirected complex networks.

Recent advances in network controllability extend beyond foundational state and structural controllability, addressing increasingly complex challenges. Key research directions include nonlinear networks [15], where progress in Lyapunov methods and basin-of-attraction analyses has enhanced stability control and feasibility for complex systems such as gene regulatory and ecological networks. Temporal and time-varying networks, with evolving connections in transportation and communication systems, require time-varying dynamic frameworks [16] and higher-order models to capture the impact of time-dependent interactions on the network controllability [17]. Energy-efficient control, critical for large-scale or resource-constrained networks [18], focuses on optimizing the number and location of driver nodes, reducing control energy, and ensuring robustness using fault-tolerant strategies for infrastructures such as power grids and cyber-physical networks. In addition, new directions include targeted control of specific nodes [19] and control of multi-relational and multilayer networks [20], all emphasizing practical applications and experimental verification to ensure scalability and real-world relevance.

Among the above key topics, a particular important and fundamental issue in network controllability is *robustness*, which raises two central research questions to be addressed by this book:

- *How can complex networks maintain intended functionality under structural failures and attacks?*
- *How can this capability be evaluated, analyzed and optimized?*

Structural disruptions can result from random failures such as natural disaster events, aging components, and unforeseen breakdowns, as well as from deliberate malicious attacks including cyber destruction and sabotage, often targeting critical nodes or edges to maximize the effect and impact. Ensuring robustness is thus essential for reliable operations of critical systems such as power grids, communication networks, and transportation infrastructure under uncertain and adversarial conditions.

Recently, on the other hand, machine learning has become a powerful tool for advancing research on network controllability and robustness. Leveraging machine learning algorithms enables efficient analysis of complex system dynamics, identification of critical nodes, and optimization of control strategies. Machine learning supports behavior modeling, pattern discovery, adaptive control, and higher-dimensional network analysis, accelerating solutions and improving controllability across diverse applications. Furthermore, both attack strategies and protective measures have evolved significantly through integration of network science theory and machine learning techniques [21–26]. Addressing these challenges is crucial for designing resilient and secure systems capable of maintaining functionality in dynamic and hostile environments.

1.2 Practical Applications of Controllability and Controllability Robustness

Network controllability has wide-ranging applications. In neuroscience, controllability aids in understanding brain activities and influencing regions for therapy [27]. In power systems, controllability supports the design of resilient grids for stability and fault recovery [28]. In transportation networks, controllability optimizes routes, traffic flow, and resource allocation for efficient operations [29]. Without controllability, a system may fail to respond effectively to control inputs, leading to degraded performance or instability.

Recent research has advanced network controllability across diverse topological types and configurations [4, 5]. In multiplex and multilayer

networks, controllability is influenced by interlayer coupling and timescale differences. Control is more efficient when applied to the faster layer, and a critical timescale threshold determines whether control is dominated by one layer or shared between layers [30]. In evolving networks, a general rule predicts changes in the number of driver nodes during network growth, helping maintain controllability as new nodes and edges are added [31]. Regarding input-output configurations, comparative studies show that MIMO (multiple input multiple output) systems significantly outperform SISO (single input single output), SIMO (single input multiple output), and MISO (multiple input single output) systems in terms of channel capacity and reliability, making them ideal for high-performance communication and control systems [14,32,33]. While these improvements enhance control efficiency of a network, the structural controllability remains primarily determined by its topology.

Investigating network controllability focuses on analyzing the ability of a networked system, for those both already exist in the real world or are intended for future deployment, to be effectively fully controlled, while investigating controllability robustness extends this analysis by assessing the ability of such controllability under non-ideal conditions and in adversarial environments, ensuring its sustainability and maintenance.

Controllability robustness is essential for guaranteeing stable and continuous functionality, enabling fault recovery, and enhancing resilience, as it characterizes the capacity of a system to preserve the controllability under structural modifications or adverse conditions. Evaluating the controllability robustness of a system before real-world deployment is essential. Under stress tests conducted in intentionally designed non-ideal environments, where failures and attacks occur sequentially, system performance is measured in terms of the remaining controllability. It is then aggregated into an overall metric of controllability robustness, typically by averaging, although alternative computation methods are possible.

1.3 Adversarial Attacks and Controllability Robustness

Malicious attacks on complex networks have become increasingly critical in modern interconnected systems. Typical examples include Internet viruses, cyber intrusions, distributed denial of service (DDoS) attacks, and ransomware targeting critical infrastructure [34]. In addition, real-world systems encounter targeted disruptions on power grids and transportation networks, coordinated attacks on sensor networks, adversarial manipula-

tion on social and communication platforms, and structural degradation in biological or ecological environments. Such disruptions can propagate across interconnected infrastructures, amplifying systemic vulnerability.

Other attack forms include data corruption, which undermines the integrity of information processed by nodes [35]; communication interference, such as jamming in wireless networks [36]; overload attacks, where specific nodes or edges are intentionally stressed to induce systemic failures [37], and cascading failures, where an initial disruption propagates through the network, triggering a chain reaction of malfunctions [38]. Cyber attacks on power grids exemplify these risks, demonstrating the potential to cause large-scale blackouts and cascading crashes across interconnected facilities [39, 40]. The accelerating digitalization of power systems further enlarges the attack surface, heightening exposure to advanced persistent threats and coordinated intrusions [41]. Addressing these challenges from a general topological perspective is essential, while domain-specific expertise remains indispensable for safeguarding individual systems.

When real-world infrastructures are modeled as complex networks, their entities, such as power stations in power grids, routers and switches in communication systems, intersections and stations in transportation networks, or individuals in social networks, are represented as nodes (also called vertices), and their relationships, such as transmission lines, data links, traffic routes, or social interactions and acquaintanceship, are represented as edges (or links).

Malicious attacks, random failures, traffic congestion, dissolution of social relationships, and other environmental disturbances that alter network structures are commonly modeled by node removal or edge removal. In these scenarios, the focus extends beyond the physical nature of the damage to emphasize its structural and functional implications for the network.

Attacks on complex networks can be categorized along several dimensions. First, based on the target, they can be classified as node attacks, which aim to disable specific entities, and edge attacks, which seek to disrupt the connections among the entities. Second, according to the selection strategies, attacks may be random where nodes or edges are removed without preference, or targeted where the deemed most critical components are deliberately chosen to maximize the disruption. Third, depending on whether the importance of nodes or edges is updated during the attack process, attacks may be metric-reevaluated where the importance is recalculated after each removal, or metric-non-reevaluated where the initial ranking remains fixed. Finally, based on the methods used to assess

importance, attacks may be categorized as statistics-based which rely on metrics such as degree or betweenness, computational intelligence-based which employ heuristic algorithms such as evolutionary computation or swarm intelligence, and machine learning-based which leverage models such as graph neural networks and deep learning to identify key components automatically [42].

From an adversarial perspective, the advancement of computational intelligence and machine learning techniques has rendered both attack design and identification of critical components in complex networks increasingly adaptive and sophisticated. These developments enable adversaries to formulate precise and effective strategies, while simultaneously providing defenders with advanced tools for vulnerability detection and for implementing protective measures with greater accuracy and efficiency. Similarly, from the perspective of safeguarding networked systems, these advancements can be leveraged to strengthen the robustness and resilience, improve fault recoveries, and ensure reliable operations subject to evolving threats.

1.4 Motivation and Outline of the Book

Nowadays, as real-world environments become increasingly complex and life-threatening, robustness in network controllability has emerged as an important research focal issue. Progressively, robustness studies encompassing theoretical, computational and data-driven tasks have reached out to cover many other network functionalities such as connectivity and communication, which have contributed to the development of network science and technology.

This book addresses the fundamental challenge of assessing and enhancing network controllability robustness and provides insights into related topics, including robustness of additional network functionalities, graph learning with emphasis on performance evaluation, attack and defense strategies targeting network functionalities, and modeling random processes of malicious attacks on networks, among others.

1.4.1 *Motivation*

The rapid expansion of interconnected systems across natural, engineering, social, and biological domains has profoundly transformed their complexity to be perceived and managed in real-world applications. These networks deliver significant benefits to societies in terms of efficiency and connectivity.

Among their many functionalities and advantages, controllability is particularly important, meanwhile these systems also introduce substantial vulnerabilities. Malicious attacks, cascading failures, and unpredictable disruptions underscore the urgent need for resilient and intelligent control strategies of complex networks.

At the same time, breakthroughs in computational intelligence, particularly in graph learning, a specialized branch of machine learning that processes data represented as graph structures, and data-driven modeling, have created unprecedented opportunities to analyze, understand and optimize complex networks. These technologies provide effective tools for network analysis and computation, enabling discovery of hidden structures, evaluation of dynamic performance and behaviors, and development of adaptive solutions that respond effectively to evolving conditions.

This book is motivated by the need to bridge theoretical insights in network controllability with simulation-based studies and practical applications across diverse domains, by incorporating advances in graph learning approaches and using tools from data-driven methodologies. A unified framework for controllability robustness analysis is introduced, integrating analytical, simulation-based, and data-driven approaches for measurement and analysis, together with optimization using computational intelligence techniques. This self-contained framework provides an efficient in-depth exploration of controllability, robustness, resilience, and adaptability in complex networks.

By integrating graph theory, optimization techniques, and machine learning algorithms, this book equips readers with useful tools to address real-world challenges in network functionality robustness. The content begins with foundational concepts and progresses through theoretical analysis, practical strategies for robustness evaluation and enhancement, applications of machine learning, and future research directions. This book is intended for researchers, practitioners and students in network science, control theory, optimization, AI-assisted systems engineering, and related fields. The goal is to provide readers with a comprehensive understanding of the structural and functional properties of complex networks and to enable the design, analysis and control of these systems in an increasingly interconnected and dynamic environment, with emphasis on network controllability and its robustness.

1.4.2 *Outline of the Book*

This book is structured into seven chapters, each focusing on a specific aspect of network controllability and its robustness. The remainder of the monograph is organized as follows:

- Chapter 2 introduces the basic concept and knowledge of network controllability, covering definitions, computational methods, and evaluation metrics. The chapter analyzes controllability across synthetic and real-world networks, explores key topological features, and distinguishes the controllability robustness from the connectivity robustness.
- Chapter 3 analyzes the controllability robustness in complex networks, introducing key metrics, attack strategies, hierarchical attack methods, simulation criteria, and analytical models. Comparative studies on synthetic and real-world networks will be performed to reveal how topology and heterogeneity influence resilience of complex networks.
- Chapter 4 explores techniques for enhancing the controllability robustness, introducing robustness-oriented models, metaheuristic-based optimization, and an empirical necessary condition verified through extensive experiments. The chapter demonstrates that edge rectification transforms networks toward highly homogeneous structures, providing a practical pathway for improved network robustness in design and applications.
- Chapter 5 examines data-driven approaches for evaluating the controllability robustness, focusing on input representation, model architecture, and output interpretation. Experiments are performed to show that structure-preserving representations and advanced graph neural network (GNN) models deliver the most accurate and reliable performances compared to other approaches.
- Chapter 6 introduces a framework for assessing and visualizing the controllability robustness enhancement potential, leveraging data-driven methods to deliver accurate predictions and the interpretability at significantly lower computational cost, compared to state-of-the-art approaches.
- Chapter 7 reviews recent advancements, identifies key challenges, and outlines future directions in network controllability robustness studies, emphasizing analytical foundations, simulation frameworks, and enhancement strategies.

Bibliography

[1] G. Chen, X. F. Wang and X. Li, *Fundamentals of Complex Networks: Models, Structures and Dynamics*, 2nd edn. John Wiley & Sons (2014).
[2] A.-L. Barabási, *Network Science*. Cambridge University Press (2016).
[3] M. E. Newman, *Networks*, 2nd edn. Oxford University Press (2018).
[4] L. Xiang, F. Chen, W. Ren and G. Chen, Advances in network controllability, *IEEE Circuits and Systems Magazine* **19**, 2, pp. 8–32 (2019).
[5] Y. Lou, L. Wang and G. Chen, Toward robust network controllability: Insights and future directions, *Europhysics Letters* **149**, 4, p. 41003 (2025).
[6] G. Chen, Pinning control and synchronization on complex dynamical networks, *International Journal of Control, Automation and Systems* **12**, 2, pp. 221–230 (2014).
[7] E. D. Sontag, Kalman's controllability rank condition: From linear to nonlinear, in *Mathematical System Theory*. Springer, pp. 453–462 (1991).
[8] C.-T. Chen, *Linear System Theory and Design*, 3rd edn. Oxford University Press (1998).
[9] Z. Z. Yuan, C. Zhao, Z. R. Di, W.-X. Wang and Y.-C. Lai, Exact controllability of complex networks, *Nature Communications* **4**, p. 2447 (2013).
[10] Y.-Y. Liu, J.-J. Slotine and A.-L. Barabási, Controllability of complex networks, *Nature* **473**, 7346, pp. 167–173 (2011).
[11] F. Pasqualetti, S. Zampieri and F. Bullo, Controllability metrics, limitations and algorithms for complex networks, *IEEE Transactions on Control of Network Systems* **1**, 1, pp. 40–52 (2014).
[12] C. W. Wu, Synchronization and convergence of linear dynamics in random directed networks, *IEEE Transactions on Automatic Control* **51**, 7, pp. 1207–1210 (2006).
[13] X. F. Wang, X. Li and J. Lu, Control and flocking of networked systems via pinning, *IEEE Circuits and Systems Magazine* **10**, 3, pp. 83–91 (2010).
[14] G. Chen, Pinning control and controllability of complex dynamical networks, *International Journal of Automation and Computing* **14**, pp. 1–9 (2017).
[15] J. Jiang and Y.-C. Lai, Irrelevance of linear controllability to nonlinear dynamical networks, *Nature Communications* **10**, 1, p. 3961 (2019).

[16] L. C. G. Lebon, F. L. Iudice and C. Altafini, On controllability of temporal networks, *European Journal of Control* **80** (2024).

[17] Y. Zhang, A. Garas and I. Scholtes, Higher-order models capture changes in controllability of temporal networks, *Journal of Physics: Complexity* **2**, 1, p. 015007 (2021).

[18] C. Hou, Energy-efficient control of multiple smart sensors with uncertain controllability, *IEEE Transactions on Automation Science and Engineering* (2024).

[19] J. Gao, Y.-Y. Liu, R. M. D'souza and A.-L. Barabási, Target control of complex networks, *Nature Communications* **5**, 1, pp. 1–8 (2014).

[20] L. Wang, Z. Li, L. Cao, G. Guo and Z. Kong, Controllability of multi-relational networks with heterogeneous dynamical nodes, *IEEE/CAA Journal of Automatica Sinica* **11**, 12, pp. 2476–2486 (2024).

[21] C. Fan, L. Zeng, Y. Sun and Y.-Y. Liu, Finding key players in complex networks through deep reinforcement learning, *Nature Machine Intelligence* **2**, pp. 317–324 (2020).

[22] Y. Lou, Y. He, L. Wang and G. Chen, Predicting network controllability robustness: A convolutional neural network approach, *IEEE Transactions on Cybernetics* **52**, 5, pp. 4052–4063 (2022).

[23] A. Said, O. U. Ahmad, W. Abbas, M. Shabbir and X. Koutsoukos, Network controllability perspectives on graph representation, *IEEE Transactions on Knowledge and Data Engineering* **36**, 8, pp. 4116–4127 (2024).

[24] Y. Zhang, J. Li, J. Ding and X. Li, A graph transformer-driven approach for network robustness learning, *IEEE Transactions on Circuits and Systems I: Regular Papers* **71**, 5, pp. 1992–2005 (2024a).

[25] Y. Zhang, J. Ding and X. Li, Network controllability robustness learning via spatial graph neural networks, *IEEE Transactions on Network Science and Engineering* **11**, 5, pp. 4045–4058 (2024b).

[26] Y. Lou, C. Wu, L. Chen, W. Huang, L. Zhou, L. Wang and G. Chen, Exploring the potential for enhancing structural robustness of complex networks, *IEEE Computational Intelligence Magazine* **20**, 4 (2025).

[27] S. Gu, F. Pasqualetti, M. Cieslak, Q. K. Telesford, A. B. Yu, A. E. Kahn, J. D. Medaglia, J. M. Vettel, M. B. Miller, S. T. Grafton and D. S. Bassett, Controllability of structural brain networks, *Nature Communications* **6**, p. 8414 (2015).

[28] Z. Chen, X. Zhou, Z. Liu, R. Zeng, X. Gong, X. Wu and F. Tang, Impedance network model based modal observability and controllability analysis for renewable integrated power systems, *IEEE Transactions on Power Systems* **35**, 3, pp. 1853–1865 (2020).

[29] M. Rinaldi, Controllability of transportation networks, *Transportation Research Part B: Methodological* **118**, pp. 381–406 (2018).

[30] M. Pósfai, J. Gao, S. P. Cornelius, A.-L. Barabási and R. M. D'Souza, Controllability of multiplex, multi-time-scale networks, *Physical Review E* **94**, 3, p. 032316 (2016).

[31] R. Zhang, X. Wang, M. Cheng and T. Jia, The evolution of network controllability in growing networks, *Physica A: Statistical Mechanics and Its Applications* **520**, pp. 257–266 (2019).

[32] L. Wang, X. F. Wang, G. Chen and W. K. S. Tang, Controllability of networked MIMO systems, *Automatica* **69**, pp. 405–409 (2016).
[33] M. R. Rahmati and G. Flores, On brunovsky numbers and observability and controllability indices in nonlinear mimo systems, *SIAM Journal on Control and Optimization* **63**, 2, pp. 1485–1513 (2025).
[34] Z. Xie, Y. Su, G. Liu, Y. Yang and P. Arebi, Dynamical repair strategy of data network controllability processes against DoS attack on complex temporal networks, *Peer-to-Peer Networking and Applications* **18**, pp. 1–15 (2025).
[35] E. Ortiz-Ospina and M. Roser, Corruption, https://ourworldindata.org/corruption (2024), accessed: 2024-01-03.
[36] B. Gu, D. Li, H. Ding, G. Wang and C. Tellambura, Breaking the interference and fading gridlock in backscatter communications: State-of-the-art, design challenges, and future directions, *IEEE Communications Surveys & Tutorials* (2024), doi:10.1109/COMST.2024.3436082.
[37] E.-C. Chen, P.-Y. Chen, I.-H. Chung and C.-R. Lee, Overload: Latency attacks on object detection for edge devices, in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 24716–24725 (2024).
[38] N. M. Sami and M. Naeini, Machine learning applications in cascading failure analysis in power systems: A review, *Electric Power Systems Research* **210**, p. 108024 (2024).
[39] U.S. Government Accountability Office, Securing the u.s. electricity grid from cyberattacks, https://www.gao.gov/blog/securing-u.s.-electricity-grid-cyberattacks (2022), accessed: 2025-08-26.
[40] K. Ayano, Cybersecurity in critical infrastructure: Protecting power grids and smart grids, (2024), https://www.cyberdefensemagazine.com/cybersecurity-in-critical-infrastructure-protecting-power-grids-and-smart-grids, accessed: 2025-08-26.
[41] T. Krause, R. Ernst, B. Klaer, I. Hacker and M. Henze, Cybersecurity in power grids: Challenges and opportunities, *Sensors* **21**, 18, p. 6225 (2021).
[42] Y. Lou, L. Wang and G. Chen, Structural robustness of complex networks: A survey of *a posteriori* measures, *IEEE Circuits and Systems Magazine* **23**, 1, pp. 12–35 (2023).
[43] R. E. Kalman, Mathematical description of linear dynamical systems, *Journal of the Society for Industrial and Applied Mathematics, Series A: Control* **1**, 2, pp. 152–192 (1963).
[44] C. K. Chui and G. Chen, *Linear Systems and Optimal Control*. Springer-Verlag Berlin Heidelberg (1989).
[45] N. Jacobson, *Lie Algebras*. Courier Corporation (2013).
[46] M. L. J. Hautus, Controllability and observability conditions of linear autonomous systems, in *Indagationes Mathematicae (Proceedings)*, Vol. 72, pp. 443–448 (1969).
[47] C.-T. Lin, Structural controllability, *IEEE Transactions on Automatic Control* **19**, 3, pp. 201–208 (1974).

[48] A. Y. Yazıcıoğlu, W. Abbas and M. Egerstedt, Graph distances and controllability of networks, *IEEE Transactions on Automatic Control* **61**, 12, pp. 4125–4130 (2016).

[49] P. Erdös and A. Rényi, On the strength of connectedness of a random graph, *Acta Mathematica Hungarica* **12**, 1-2, pp. 261–267 (1964).

[50] Y. Lou, L. Wang, K.-F. Tsang and G. Chen, Towards optimal robustness of network controllability: An empirical necessary condition, *IEEE Transactions on Circuits and Systems I: Regular Papers* **67**, 9, pp. 3163–3174 (2020).

[51] A.-L. Barabási and R. Albert, Emergence of scaling in random networks, *Science* **286**, 5439, pp. 509–512 (1999).

[52] C.-L. Pu, W.-J. Pei and A. Michaelson, Robustness analysis of network controllability, *Physica A: Statistical Mechanics and its Applications* **391**, 18, pp. 4420–4425 (2012).

[53] K.-I. Goh, B. Kahng and D. Kim, Universal behavior of load distribution in scale-free networks, *Physical Review Letters* **87**, 27, p. 278701 (2001).

[54] F. Sorrentino, Effects of the network structural properties on its controllability, *Chaos: An Interdisciplinary Journal of Nonlinear Science* **17**, 3, p. 033101 (2007).

[55] D. J. Watts and S. H. Strogatz, Collective dynamics of 'small-world' networks, *Nature* **393**, 6684, pp. 440–442 (1998).

[56] M. E. Newman and D. J. Watts, Renormalization group analysis of the small-world network model, *Physics Letters A* **263**, 4-6, pp. 341–346 (1999).

[57] G. Chen, Y. Lou and L. Wang, A comparative study on controllability robustness of complex networks, *IEEE Transactions on Circuits and Systems II: Express Briefs* **66**, 5, pp. 828–832 (2019).

[58] Y. Lou, L. Wang and G. Chen, Toward stronger robustness of network controllability: A snapback network model, *IEEE Transactions on Circuits and Systems I: Regular Papers* **65**, 9, pp. 2983–2991 (2018).

[59] Y. Lou, L. Wang and G. Chen, Enhancing controllability robustness of q-snapback networks through redirecting edges, *Research* **2019**, 7857534 (2019).

[60] J. Leskovec, L. Backstrom, R. Kumar and A. Tomkins, Microscopic evolution of social networks, in *International Conference on Knowledge Discovery and Data Mining*, pp. 462–470 (2008).

[61] J. Ugander, B. Karrer, L. Backstrom and C. Marlow, The anatomy of the facebook social graph, *arXiv preprint arXiv:1111.4503* (2011).

[62] Y. Lou, D. Yang, L. Wang, C. Tang and G. Chen, Controllability robustness of henneberg-growth complex networks, *IEEE Access* **10**, pp. 5103–5114 (2022).

[63] B. Rozemberczki, O. Kiss and R. Sarkar, Karate club: an api oriented open-source python framework for unsupervised learning on graphs, in *ACM International Conference on Information and Knowledge Management*, pp. 3125–3132 (2020).

[64] K. M. Borgwardt, C. S. Ong, S. Schönauer, S. Vishwanathan, A. J. Smola and H.-P. Kriegel, Protein function prediction via graph kernels, *Bioinformatics* **21**, suppl_1, pp. i47–i56 (2005).

[65] P. D. Dobson and A. J. Doig, Distinguishing enzyme structures from non-enzymes without alignments, *Journal of Molecular Biology* **330**, 4, pp. 771–783 (2003).

[66] P. Yanardag and S. Vishwanathan, Deep graph kernels, in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1365–1374 (2015).

[67] G. Menichetti, L. Dall'Asta and G. Bianconi, Network controllability is determined by the density of low in-degree and out-degree nodes, *Physical Review Letters* **113**, 7, p. 078701 (2014).

[68] X.-Y. Yan, W.-X. Wang, G. Chen and D. Shi, Multiplex congruence network of natural numbers, *Scientific Reports* **6**, p. 23714 (2016).

[69] T. Österlund, S. Bordel and J. Nielsen, Controllability analysis of transcriptional regulatory networks reveals circular control patterns among transcription factors, *Integrative Biology* **7**, 5, pp. 560–568 (2015).

[70] J. Li, L. Dueñas-Osorio, C. Chen, B. Berryhill and A. Yazdani, Characterizing the topological and controllability features of US power transmission networks, *Physica A: Statistical Mechanics and Its Applications* **453**, pp. 84–98 (2016).

[71] C. M. Schneider, A. A. Moreira, J. S. Andrade, S. Havlin and H. J. Herrmann, Mitigation of malicious attacks on networks, *Proceedings of the National Academy of Sciences* **108**, 10, pp. 3838–3841 (2011).

[72] Y. Lou, R. Wu, J. Li, L. Wang and G. Chen, A convolutional neural network approach to predicting network connectedness robustness, *IEEE Transactions on Network Science and Engineering* **8**, 4, pp. 3209–3219 (2021).

[73] M. Cremonini and F. Casamassima, Controllability of social networks and the strategic use of random information, *Computational Social Networks* **4**, pp. 1–22 (2017).

[74] Q. Miao, Z. Rong, Y. Tang and J. Fang, Effects of degree correlation on the controllability of networks, *Physica A: Statistical Mechanics and Its Applications* **387**, 24, pp. 6225–6230 (2008).

[75] H. J. Herrmann, C. M. Schneider, A. A. Moreira, J. S. Andrade Jr and S. Havlin, Onion-like network topology enhances robustness against malicious attacks, *Journal of Statistical Mechanics: Theory and Experiment* **2011**, 01, p. P01027 (2011).

[76] Y.-Y. Liu, J.-J. Slotine and A.-L. Barabási, Control centrality and hierarchical structure in complex networks, *PLoS One* **7**, 9, p. e44459 (2012).

[77] H. Chan and L. Akoglu, Optimizing network robustness by edge rewiring: A general framework, *Data Mining and Knowledge Discovery* **30**, 5, pp. 1395–1425 (2016).

[78] S. Freitas, D. Yang, S. Kumar, H. Tong and D. H. Chau, Graph vulnerability and robustness: A survey, *IEEE Transactions on Knowledge and Data Engineering* **35**, 6, pp. 5915–5934 (2023).

[79] S. Wang, J. Liu and Y. Jin, Surrogate-assisted robust optimization of large-scale networks based on graph embedding, *IEEE Transactions on Evolutionary Computation* **24**, 4, pp. 735–749 (2020).

[80] S. Wang, J. Liu and Y. Jin, A computationally efficient evolutionary algorithm for multiobjective network robustness optimization, *IEEE Transactions on Evolutionary Computation* **25**, 3, pp. 419–432 (2021).

[81] U. Usman, A. Mahmood and L. Wang, Robust control centrality, *2019 Chinese Control Conference* , pp. 5486–5491 (2019).

[82] D. Parekh, D. Ruths and J. Ruths, Reachability-based robustness of network controllability under node and edge attacks, in *International Conference on Signal-Image Technology and Internet-Based Systems*. IEEE, pp. 424–431 (2014).

[83] P. Sun, R. E. Kooij and P. Van Mieghem, Reachability-based robustness of controllability in sparse communication networks, *IEEE Transactions on Network and Service Management* (2021).

[84] B. R. da Cunha, J. C. Gonzalez-Avella and S. Goncalves, Fast fragmentation of networks using module-based attacks, *PLoS One* **10**, 11 (2015).

[85] S. Shai, D. Y. Kenett, Y. N. Kenett, M. Faust, S. Dobson and S. Havlin, Critical tipping point distinguishing two types of transitions in modular network structures, *Physical Review E* **92**, 6, p. 062805 (2015).

[86] X.-L. Ren, N. Gleinig, D. Helbing and N. Antulov-Fantulin, Generalized network dismantling, *Proceedings of the National Academy of Sciences* **116**, 14, pp. 6554–6559 (2019).

[87] M. Engsig, A. Tejedor, Y. Moreno, E. Foufoula-Georgiou and C. Kasmi, Domirank centrality reveals structural fragility of complex networks via node dominance, *Nature Communications* **15**, 1, p. 56 (2024).

[88] T. Nie, Z. Guo, K. Zhao and Z.-M. Lu, New attack strategies for complex networks, *Physica A: Statistical Mechanics and Its Applications* **424**, pp. 248–253 (2015).

[89] Z.-M. Lu and X.-F. Li, Attack vulnerability of network controllability, *PLoS One* **11**, 9 (2016).

[90] H. Wang, J. Huang, X. Xu and Y. Xiao, Damage attack on complex networks, *Physica A: Statistical Mechanics and Its Applications* **408**, pp. 134–148 (2014).

[91] Y. Lou, L. Wang and G. Chen, A framework of hierarchical attacks to network controllability, *Communications in Nonlinear Science and Numerical Simulation* **98**, p. 105780 (2021).

[92] P. Sun, R. E. Kooij, Z. He and P. Van Mieghem, Quantifying the robustness of network controllability, in *International Conference on System Reliability and Safety*. IEEE, pp. 66–76 (2019).

[93] A. Braunstein, L. Dall'Asta, G. Semerjian and L. Zdeborová, Network dismantling, *Proceedings of the National Academy of Sciences* **113**, 44, pp. 12368–12373 (2016).

[94] A. E. Eiben and J. E. Smith, From evolutionary computation to the evolution of things, *Nature* **521**, pp. 476–482 (2015).

[95] D. H. Wolpert and W. G. Macready, No free lunch theorems for optimization, *IEEE Transactions on Evolutionary Computation* **1**, 1, pp. 67–82 (1997).

[96] M. Grassia, M. De Domenico and G. Mangioni, Machine learning dismantling and early-warning signals of disintegration in complex systems, *Nature Communications* **12**, 5190 (2021).

[97] A. Dhiman, P. Sun and R. Kooij, Using machine learning to quantify the robustness of network controllability, in *International Conference on Machine Learning for Networking*. Springer, pp. 19–39 (2021).

[98] Y. Lou, Y. He, L. Wang, K. F. Tsang and G. Chen, Knowledge-based prediction of network controllability robustness, *IEEE Transactions on Neural Networks and Learning Systems* **33**, 10, pp. 5739–5750 (2022).

[99] J. Yan, H. He, X. Zhong and Y. Tang, Q-learning-based vulnerability analysis of smart grid against sequential topology attacks, *IEEE Transactions on Information Forensics and Security* **12**, 1, pp. 200–210 (2016).

[100] O. Lordan and M. Albareda-Sambola, Exact calculation of network robustness, *Reliability Engineering & System Safety* **183**, pp. 276–280 (2019).

[101] C. Wu, Y. Lou, J. Li, L. Wang, S. Xie and G. Chen, A multitask network robustness analysis system based on the graph isomorphism network, *IEEE Transactions on Cybernetics* **54**, 11, pp. 6630–6642 (2024).

[102] Q. Cai, S. Alam, M. Pratama and J. Liu, Robustness evaluation of multipartite complex networks based on percolation theory, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **51**, 10, pp. 6244–6257 (2021).

[103] Y. Lou, L. Wang, S. Xie and G. Chen, Approximating the controllability robustness of directed random-graph networks against random edge-removal attacks, *International Journal of Control, Automation and Systems* **21**, 2, pp. 376–388 (2023).

[104] E. N. Gilbert, Random graphs, *The Annals of Mathematical Statistics* **30**, 4, pp. 1141–1144 (1959).

[105] P. Erdös and A. Rényi, On the evolution of random graphs, *Mathematical Institute of the Hungarian Academy of Sciences* **5**, pp. 17–61 (1960).

[106] D. Shizuka and D. R. Farine, Measuring the robustness of network community structure using assortativity, *Animal Behaviour* **112**, pp. 237–246 (2016).

[107] J. Wu, M. Barahona, Y.-J. Tan and H.-Z. Deng, Spectral measure of structural robustness in complex networks, *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* **41**, 6, pp. 1244–1252 (2011).

[108] M. Pósfai, Y.-Y. Liu, J.-J. Slotine and A.-L. Barabási, Effect of correlations on network controllability, *Scientific Reports* **3**, p. 1067 (2013).

[109] E. Wu-Yan, R. F. Betzel, E. Tang, S. Gu, F. Pasqualetti and D. S. Bassett, Benchmarking measures of network controllability on canonical graph models, *Journal of Nonlinear Science* , pp. 1–39 (2018).

[110] Y. Hao, Z. Duan and G. Chen, Further on the controllability of networked MIMO LTI systems, *International Journal of Robust and Nonlinear Control* **28**, 5, pp. 1778–1788 (2018).

[111] P. Holme, B. J. Kim, C. N. Yoon and S. K. Han, Attack vulnerability of complex networks, *Physical Review E* **65**, 5, p. 056109 (2002).

[112] B. Shargel, H. Sayama, I. R. Epstein and Y. Bar-Yam, Optimization of robustness and connectivity in complex networks, *Physical Review Letters* **90**, 6, p. 068701 (2003).

[113] A. Bashan, Y. Berezin, S. Buldyrev and S. Havlin, The extreme vulnerability of interdependent spatially embedded networks, *Nature Physics* **9**, pp. 667–672 (2013).

[114] Y.-D. Xiao, S.-Y. Lao, L.-L. Hou and L. Bai, Optimization of robustness of network controllability against malicious attacks, *Chinese Physics B* **23**, 11, p. 118902 (2014).

[115] S. Wang and J. Liu, A multi-objective evolutionary algorithm for promoting the emergence of cooperation and controllable robustness on directed networks, *IEEE Transactions on Network Science and Engineering* **5**, 2, pp. 92–100 (2018).

[116] L. Bai, Y.-D. Xiao, L.-L. Hou and S.-Y. Lao, Smart rewiring: Improving network robustness faster, *Chinese Physics Letters* **32**, 7, p. 078901 (2015).

[117] K. Yamashita, Y. Yasuda, R. Nakamura and H. Ohsaki, On the predictability of network robustness from spectral measures, in *2019 IEEE 43rd Annual Computer Software and Applications Conference*, Vol. 2. IEEE, pp. 24–29 (2019).

[118] L. Hou, S. Lao, B. Jiang and L. Bai, Enhancing complex network controllability by rewiring links, in *International Conference on Intelligent System Design and Engineering Applications*. IEEE, pp. 709–711 (2013).

[119] J. Xu, J. Wang, H. Zhao and S. Jia, Improving controllability of complex networks by rewiring links regularly, in *Chinese Control and Decision Conference*, pp. 642–645 (2014).

[120] J. Liu, H. A. Abbass and K. C. Tan, Evolving robust networks using evolutionary algorithms, in *Evolutionary Computation and Complex Networks*. Springer, pp. 117–140 (2019).

[121] S. Wang and J. Liu, Designing comprehensively robust networks against intentional attacks and cascading failures, *Information Sciences* **478**, pp. 125–140 (2019).

[122] R. C. Gunasekara, C. K. Mohan and K. Mehrotra, Multi-objective optimization to improve robustness in networks, in *Multi-Objective Optimization*. Springer, pp. 115–139 (2018).

[123] A. Zeng and W. Liu, Enhancing network robustness against malicious attacks, *Physical Review E* **85**, 6, p. 066130 (2012).

[124] Z.-X. Wu and P. Holme, Onion structure and network robustness, *Physical Review E* **84**, 2, p. 026106 (2011).

[125] T. Tanizawa, S. Havlin and H. E. Stanley, Robustness of onionlike correlated networks against targeted attacks, *Physical Review E* **85**, 4, p. 046109 (2012).

[126] Y. Hayashi and N. Uchiyama, Onion-like networks are both robust and resilient, *Scientific Reports* **8** (2018).

[127] L. Ma, J. Liu and B. Duan, Evolution of network robustness under continuous topological changes, *Physica A: Statistical Mechanics and Its Applications* **451**, pp. 623–631 (2016).

[128] D. Yang, M. Liu, Y. Zhang, D. Lin, Z. Fan and G. Chen, Henneberg growth of social networks: Modeling the facebook, *IEEE Transactions on Network Science and Engineering* **7**, 2, pp. 701–712 (2018).

[129] P. Buesser, F. Daolio and M. Tomassini, Optimizing the robustness of scale-free networks with simulated annealing, in *International Conference on Adaptive and Natural Computing Algorithms*. Springer, pp. 167–176 (2011).

[130] T. P. Peixoto and S. Bornholdt, Evolution of robust network topologies: Emergence of central backbones, *Physical Review Letters* **109**, 11, p. 118703 (2012).

[131] R. Fletcher, *Practical Methods of Optimization*. John Wiley & Sons (2013).

[132] X.-B. Cao, C. Hong, W.-B. Du and J. Zhang, Improving the network robustness against cascading failures by adding links, *Chaos, Solitons & Fractals* **57**, pp. 35–40 (2013).

[133] M. Zhou and J. Liu, A memetic algorithm for enhancing the robustness of scale-free networks against malicious attacks, *Physica A: Statistical Mechanics and Its Applications* **410**, pp. 131–143 (2014).

[134] L. Bai, Y.-D. Xiao, L.-L. Hou and S.-Y. Lao, Smart rewiring: Improving network robustness faster, *Chinese Physics Letters* **32**, 7, p. 078901 (2015).

[135] Y. Yang, Z. Li, Y. Chen, X. Zhang and S. Wang, Improving the robustness of complex networks with preserving community structure, *PLoS One* **10**, 2, p. e0116551 (2015).

[136] X. Tang, J. Liu and M. Zhou, Enhancing network robustness against targeted and random attacks using a memetic algorithm, *EPL (Europhysics Letters)* **111**, 3, p. 38005 (2015).

[137] S.-w. Sun, Y.-l. Ma, R.-q. Li, L. Wang and C.-y. Xia, Tabu search enhances network robustness under targeted attacks, *Physica A: Statistical Mechanics and Its Applications* **446**, pp. 82–91 (2016).

[138] X. Tang, J. Liu and X. Hao, Mitigate cascading failures on networks using a memetic algorithm, *Scientific Reports* **6**, 1, pp. 1–12 (2016).

[139] J. Park and S. G. Hahn, Bypass rewiring and robustness of complex networks, *Physical Review E* **94**, 2, p. 022310 (2016).

[140] L.-Z. Wang, Y.-Z. Chen, W.-X. Wang and Y.-C. Lai, Physical controllability of complex networks, *Scientific Reports* **7**, p. 40198 (2017).

[141] S. Wang and J. Liu, A multi-agent genetic algorithm for improving the robustness of communities in complex networks against attacks, in *2017 IEEE Congress on Evolutionary Computation*. IEEE, pp. 17–22 (2017).

[142] L. Ma, M. Gong, Q. Cai and L. Jiao, Enhancing community integrity of networks against multilevel targeted attacks, *Physical Review E* **88**, 2, p. 022810 (2013).

[143] S. Wang, J. Liu and X. Wang, Mitigation of attacks and errors on community structure in complex networks, *Journal of Statistical Mechanics: Theory and Experiment* **2017**, 4, p. 043405 (2017).

[144] L. Rong and J. Liu, A heuristic algorithm for enhancing the robustness of scale-free networks based on edge classification, *Physica A: Statistical Mechanics and Its Applications* **503**, pp. 503–515 (2018).

[145] Y. Liu, X. Wang and J. Kurths, Framework of evolutionary algorithm for investigation of influential nodes in complex networks, *IEEE Transactions on Evolutionary Computation* **23**, 6, pp. 1049–1063 (2019).

[146] T. Qiu, J. Liu, W. Si and D. O. Wu, Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks, *IEEE/ACM Transactions on Networking* **27**, 3, pp. 1028–1042 (2019).

[147] Q. Cai, S. Alam, H. Ang and V. Duong, A braess's paradox inspired method for enhancing the robustness of air traffic networks, in *2020 IEEE Symposium Series on Computational Intelligence*. IEEE, pp. 798–805 (2020).

[148] Y. Lou, S. Xie and G. Chen, Searching better rewiring strategies and objective functions for stronger controllability robustness, *IEEE Transactions on Circuits and Systems II: Express Briefs* **68**, 6, pp. 2112–2116 (2021).

[149] J. Liu, M. Zhou, S. Wang and P. Liu, A comparative study of network robustness measures, *Frontiers of Computer Science* **11**, 4, pp. 568–584 (2017).

[150] B. Mburano, W. Si and W. X. Zheng, A comparative study on the variants of r metric for network robustness, in *International Symposium on Networks, Computers and Communications*. IEEE, pp. 1–6 (2021).

[151] D. Shi, G. Chen, W. W. K. Thong and X. Yan, Searching for optimal network topology with best possible synchronizability, *IEEE Circuits and Systems Magazine* **13**, 1, pp. 66–75 (2013).

[152] J. Leskovec and A. Krevl, SNAP Datasets: Stanford large network dataset collection, http://snap.stanford.edu (2014).

[153] K. Wu, P. Watters and M. Magdon-Ismail, Network classification using adjacency matrix embeddings and deep learning, in *IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining*. IEEE, pp. 299–306 (2016).

[154] K. Hegde, M. Magdon-Ismail, R. Ramanathan and B. Thapa, Network signatures from image representation of adjacency matrices: Deep/transfer learning for subgraph classification, in *International Workshop on Mining and Learning with Graphs*. London, UK, pp. 1–8 (2018).

[155] Y.-S. Kim, M. K. Kim, N. Fu, J. Liu, J. Wang and J. Srebric, Investigating the impact of data normalization methods on predicting electricity consumption in a building using different artificial neural network models, *Sustainable Cities and Society* **118**, p. 105570 (2025).

[156] H. Cai, V. W. Zheng and K. C.-C. Chang, A comprehensive survey of graph embedding: Problems, techniques, and applications, *IEEE Transactions on Knowledge and Data Engineering* **30**, 9, pp. 1616–1637 (2018).

[157] M. Niepert, M. Ahmed and K. Kutzkov, Learning convolutional neural networks for graphs, in *International Conference on Machine Learning*, pp. 2014–2023 (2016).

[158] Y. Lou, R. Wu, J. Li, L. Wang, X. Li and G. Chen, A learning convolutional neural network approach for network robustness prediction, *IEEE Transactions on Cybernetics* **53**, 7, pp. 4531–4544 (2023).

[159] B. Perozzi, R. Al-Rfou and S. Skiena, Deepwalk: Online learning of social representations, in *Proceedings of the 20th ACM SIGKDD Interna-*

tional Conference on Knowledge Discovery and Data Mining, pp. 701–710 (2014).

[160] T. Mikolov, K. Chen, G. Corrado and J. Dean, Efficient estimation of word representations in vector space, in *Proceedings of the International Conference on Learning Representations* (2013a).

[161] T. Mikolov, I. Sutskever, K. Chen, G. S. Corrado and J. Dean, Distributed representations of words and phrases and their compositionality, in *Proceedings of the Neural Information Processing Systems*, Vol. 26 (2013b).

[162] J. Tang, M. Qu, M. Wang, M. Zhang, J. Yan and Q. Mei, Line: Large-scale information network embedding, in *Proceedings of the 24th International Conference on World Wide Web*, pp. 1067–1077 (2015).

[163] A. Grover and J. Leskovec, node2vec: Scalable feature learning for networks, in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 855–864 (2016).

[164] D. Wang, P. Cui and W. Zhu, Structural deep network embedding, in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 1225–1234 (2016).

[165] L. F. Ribeiro, P. H. Saverese and D. R. Figueiredo, struc2vec: Learning node representations from structural identity, in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, pp. 385–394 (2017).

[166] C. Cai and Y. Wang, A simple yet effective baseline for non-attributed graph classification, in *Proceedings of the International Conference on Learning Representations* (2019).

[167] S. Abu-El-Haija, B. Perozzi, R. Al-Rfou and A. Alemi, Watch your step: Learning node embeddings via graph attention, in *Advances in Neural Information Processing Systems*, pp. 4575–4584 (2018).

[168] Y. Xie, Y. Ma, Z. Xu, Y. Wang, X. H. Li, Y. Wang and S. Ji, Task-agnostic graph explanations (tage), in *Advances in Neural Information Processing Systems* (2022).

[169] A. Mucherino, P. J. Papajorgji, P. M. Pardalos, A. Mucherino, P. J. Papajorgji and P. M. Pardalos, k-nearest neighbor classification, *Data Mining in Agriculture* , pp. 83–106 (2009).

[170] G. James, D. Witten, T. Hastie, R. Tibshirani *et al.*, *An Introduction to Statistical Learning*, Vol. 112. Springer (2013).

[171] J. R. Quinlan, Induction of decision trees, *Machine Learning* **1**, pp. 81–106 (1986).

[172] D. E. Rumelhart, G. E. Hinton and R. J. Williams, Learning representations by back-propagating errors, *Nature* **323**, pp. 533–536 (1986).

[173] S. Wang, J. Liu and Y. Jin, Robust structural balance in signed networks using a multiobjective evolutionary algorithm, *IEEE Computational Intelligence Magazine* **15**, 2, pp. 24–35 (2020).

[174] W. L. Hamilton, R. Ying and J. Leskovec, Inductive representation learning on large graphs, in *International Conference on Neural Information Processing Systems*, pp. 1025–1035 (2017).

[175] W. L. Hamilton, Graph representation learning, *Synthesis Lectures on Artifical Intelligence and Machine Learning* **14**, 3, pp. 1–159 (2020).

[176] M. Raissi, P. Perdikaris and G. E. Karniadakis, Physics-informed neural networks: A deep learning framework for solving forward and inverse problems involving nonlinear partial differential equations, *Journal of Computational Physics* **378**, pp. 686–707 (2019).

[177] K. He, X. Zhang, S. Ren and J. Sun, Spatial pyramid pooling in deep convolutional networks for visual recognition, *IEEE Transactions on Pattern Analysis and Machine Intelligence* **37**, 9, pp. 1904–1916 (2015).

[178] K. Grauman and T. Darrell, The pyramid match kernel: Discriminative classification with sets of image features, in *IEEE International Conference on Computer Vision*, Vol. 2. IEEE, pp. 1458–1465 (2005).

[179] S. Lazebnik, C. Schmid and J. Ponce, Beyond bags of features: Spatial pyramid matching for recognizing natural scene categories, in *IEEE Conference on Computer Vision and Pattern Recognition*, Vol. 2. IEEE, pp. 2169–2178 (2006).

[180] C. Wu, Y. Lou, L. Wang, J. Li, X. Li and G. Chen, SPP-CNN: An efficient framework for network robustness prediction, *IEEE Transactions on Circuits and Systems I: Regular Papers* **70**, 10, pp. 4067–4079 (2023).

[181] Y. Lou, R. Wu, J. Li, L. Wang, C.-B. Tang and G. Chen, Classification-based prediction of network connectivity robustness, *Neural Networks* **157**, pp. 136–146 (2023).

[182] J. Sun, W. Zheng, Q. Zhang and Z. Xu, Graph neural network encoding for community detection in attribute networks, *IEEE Transactions on Cybernetics* **52**, 8, pp. 7791–7804 (2022).

[183] Z. Wu, S. Pan, F. Chen, G. Long, C. Zhang and S. Y. Philip, A comprehensive survey on graph neural networks, *IEEE Transactions on Neural Networks and Learning Systems* **32**, 1, pp. 4–24 (2021).

[184] J. Li, Y. Ji, Y. Zhang, J. Ding, C. Li and X. Li, Graph neural networks for network science: A mini review, *Europhysics Letters* (2025).

[185] P. Veličković, Everything is connected: Graph neural networks, *Current Opinion in Structural Biology* **79**, p. 102538 (2023).

[186] J. Gilmer, S. S. Schoenholz, P. F. Riley, O. Vinyals and G. E. Dahl, Neural message passing for quantum chemistry, in *International Conference on Machine Learning*. PMLR, pp. 1263–1272 (2017).

[187] T. N. Kipf and M. Welling, Semi-supervised classification with graph convolutional networks, in *International Conference on Learning Representations* (2017).

[188] P. Veličković, G. Cucurull, A. Casanova, A. Romero, P. Lio and Y. Bengio, Graph attention networks, (2018).

[189] M. Zhang, Z. Cui, M. Neumann and Y. Chen, An end-to-end deep learning architecture for graph classification, in *AAAI Conference on Artificial Intelligence*, Vol. 32 (2018).

[190] K. Xu, C. Li, Y. Tian, T. Sonobe, K.-i. Kawarabayashi and S. Jegelka, Representation learning on graphs with jumping knowledge networks, in *International Conference on Machine Learning*. PMLR, pp. 5453–5462 (2018).

[191] K. Xu, W. Hu, J. Leskovec and S. Jegelka, How powerful are graph neural networks? in *International Conference on Machine Learning* (2019).

[192] Y. Zhang, J. Li, J. Ding and X. Li, A graph transformer-driven approach for network robustness learning, *IEEE Transactions on Circuits and Systems I: Regular Papers* **71**, 5, pp. 1992–2005 (2024).

[193] A. Kendall, Y. Gal and R. Cipolla, Multi-task learning using uncertainty to weigh losses for scene geometry and semantics, in *IEEE Conference on Computer Vision and Pattern Recognition*, pp. 7482–7491 (2018).

[194] R. Rossi and N. Ahmed, The network data repository with interactive graph analytics and visualization, in *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 29 (2015).

[195] J. Zhang, E. Modiano and D. Hay, Enhancing network robustness via shielding, *IEEE/ACM Transactions on Networking* **25**, 4, pp. 2209–2222 (2017).

[196] S. Wang, W. Lv, J. Zhang, S. Luan, C. Chen and X. Gu, Method of power network critical nodes identification and robustness enhancement based on a cooperative framework, *Reliability Engineering & System Safety* **207**, p. 107313 (2021).

[197] L. Ma, X. Zhang, J. Li, Q. Lin, M. Gong, C. A. C. Coello and A. K. Nandi, Enhancing robustness and resilience of multiplex networks against node-community cascading failures, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **52**, 6, pp. 3808–3821 (2021).

[198] M. Chujyo and F. Toriumi, Link-limited bypass rewiring for enhancing the robustness of complex networks, *Applied Network Science* **9**, 1, pp. 1–17 (2024).

[199] A. Beygelzimer, G. Grinstein, R. Linsker and I. Rish, Improving network robustness by edge modification, *Physica A: Statistical Mechanics and Its Applications* **357**, 3-4, pp. 593–612 (2005).

[200] M. Tomassini, Rewiring or adding links: A real-world case study of network vulnerability, *Physica A: Statistical Mechanics and its Applications* **630**, p. 129241 (2023).

[201] L. Katz, A new status index derived from sociometric analysis, *Psychometrika* **18**, pp. 39–43 (1953).

[202] S. Brin and L. Page, The anatomy of a large-scale hypertextual web search engine, *Computer Networks and ISDN Systems* **30**, 1-7, pp. 107–117 (1998).

[203] L. v. d. Maaten and G. Hinton, Visualizing data using t-SNE, *Journal of Machine Learning Research* **9**, 11, pp. 2579–2605 (2008).

[204] T. Kohonen, The self-organizing map, *Proceedings of the IEEE* **78**, 9, pp. 1464–1480 (1990).

[205] L. McInnes, J. Healy and J. Melville, UMAP: Uniform manifold approximation and projection for dimension reduction, *arXiv preprint arXiv:1802.03426* (2018).

[206] A.-L. Barabási, Scale-free networks: A decade and beyond, *Science* **325**, 5939, pp. 412–413 (2009).

[207] P. Misra and A. S. Yadav, Improving the classification accuracy using recursive feature elimination with cross-validation, *International Journal on Emerging Technologies* **11**, 3, pp. 659–665 (2020).

[208] S. Zhao and F. Pasqualetti, Networks with diagonal controllability gramian: Analysis, graphical conditions, and design algorithms, *Automatica* **102**, pp. 10–18 (2019).

Appendix A

Lists of Symbols, Notation, Acronyms, Abbreviations

List of Symbols and Notation

- $A_{i,j}$: Entry of adjacency matrix
- $\bar{\xi}$: Mean prediction error
- $\mathbf{A}$: System matrix
- $\mathbf{A}^{(k)}$: High-order adjacency matrix
- $\mathbf{B}$: Input/Incidence matrix
- $\mathbf{C}$: Controllability matrix
- $\mathbf{D}$: Degree matrix
- $\mathbf{H}$: Modularity matrix
- $\mathbf{L}$: Laplacian matrix
- $\mathbf{L}^*$: Laplacian matrix with one row and column removed
- $\mathbf{W}^{(\ell)}$: Weight matrix at layer ℓ
- γ: Power-law exponent
- $\lambda_{\max}$: Largest eigenvalue
- $\langle k \rangle$: Average degree
- $\langle m \rangle$: Average number of edges
- $\langle n \rangle$: Average number of nodes
- n_D: Number of driver nodes
- $\mathbb{R}$: Real number field
- $\mathcal{E}^*$: Maximum matching set
- $|\mathcal{E}^*|$: Number of edges in maximum matching
- $\mathcal{F}$: Feature/Importance metric
- $\mathcal{G}^*$: Optimal network instance
- $\hat{\mathcal{G}}^*$: Approximate optimal network
- $\mathcal{L}$: Loss function
- σ: Proportion of nodes/edges been attacked

- $\sigma(\cdot)$: Activation function
- $\xi(i)$: Error at step i
- d_{st}: Shortest-path distance between nodes s, t
- $h_v^{(\ell)}$: Node representation at layer ℓ
- $h_{\mathcal{N}_v}^{(\ell+1)}$: Aggregated neighborhood representation
- $H_{\mathcal{G}}$: Graph-level representation
- k_i: Degree of node i
- k_i^{in}: In-degree of node i
- k_i^{out}: Out-degree of node i
- L: Total number of layers
- m: Number of edges
- m_c: Number of critical edges
- n: Number of nodes
- c_D: Ratio and minimum number of driver nodes
- n_D: Minimum number of driver nodes
- $n_{\mathcal{N}}$: Number of nearest neighbors
- p_c: Connection or rewiring probability
- q: Snapback probability
- q_{QS}: Snapback probability in QS model
- r_{QS}: Layer index in QS model

List of Acronyms and Abbreviations

- ACO: Algebraic Connectivity
- APL: Average Path Length
- AST: Assortativity
- BDC: Betweenness-Clustering-Degree Embedding
- CNN: Convolutional Neural Network
- DeepWalk: Random Walk-Based Embedding Method
- DIA: Network Diameter
- DT: Decision Tree
- EFF: Efficiency
- EFR: Effective Resistance
- GAP: Spectral Gap
- GAT: Graph Attention Network
- GCN: Graph Convolutional Network
- GIN: Graph Isomorphism Network
- GNN: Graph Neural Network
- KNN: K-Nearest Neighbors

- LDP: Local Degree Profile
- LFR: Learning Feature Representation
- LINE: Large-Scale Information Network Embedding
- LR: Linear Regression
- LGC: Largest Circle
- MLP: Multi-Layer Perceptron
- MOD: Modularity
- mCNN-RP: Multi-Expert CNN Robustness Predictor
- NCO: Natural Connectivity
- NOC: Number of Circles
- NST: Number of Spanning Trees
- PATCHY-SAN: CNN-Based Graph Representation Method
- PCA: Principal Component Analysis
- PGR: PageRank
- RAD: Spectral Radius
- RF: Random Forest
- RPE: Robustness Potential Explorer
- RPE-F: Feature Extraction Module in RPE
- RPE-P: Prediction Module in RPE
- RPE-V: Visualization Module in RPE
- SDNE: Structural Deep Network Embedding
- SOM: Self-Organizing Map
- SPP: Spatial Pyramid Pooling
- struc2vec: Structural Role-Based Embedding Method
- t-SNE: t-Distributed Stochastic Neighbor Embedding
- TRA: Transitivity
- UMAP: Uniform Manifold Approximation and Projection

This page intentionally left blank

Appendix B

Lists of Figures and Tables

This page intentionally left blank

List of Figures

This page intentionally left blank

List of Tables

This page intentionally left blank

Index