J. Electrical Systems 20-3 (2024):7677-7689

Zeta Paul[1],

Jobin Varghese P[2], Alphy Jose[3],

Viji A M[4],

Josmon A J[5]

The Role of Graph Theory in Network Security: Bibliometric Insights into Research Patterns and Developments

Abstract: - This bibliometric analysis examines the role of graph theory in network security, leveraging the Scopus database to analyze research trends, significant contributors, and thematic developments in the field. Graph theory offers a robust mathematical framework for modeling networked systems, identifying vulnerabilities, and analyzing attack paths, which are crucial for enhancing resilience against cyber threats. Using Biblioshiny and VOSviewer software, this study maps out various aspects of the literature, including annual scientific production, most significant authors, and key publication sources. The findings highlight the increasing scholarly interest in this area, with a consistent growth rate reflecting the field's response to evolving cybersecurity challenges. Notable authors, sources, and highly cited documents underscore the foundational contributions that shape current research. Trend topics, such as machine learning and anomaly detection, illustrate a shift toward addressing modern threats, while a thematic map categorizes research themes by development and centrality, distinguishing between established and emerging areas. The co-occurrence analysis of keywords reveals interconnected research areas, emphasizing the multidisciplinary nature of graph theory applications in network security. Bibliographic coupling of sources shows scholarly connections and collaborative focus areas within the literature. Additionally, the co-authorship analysis of countries demonstrates strong international collaboration, with nations like China and the United Kingdom acting as central hubs. This study provides insights into the field's evolution, highlighting key research themes and collaborative networks that support advancements in network security through graph theory.

Keywords: Graph Theory, Network Security, Bibliometric Analysis, Biblioshiny, VOSviewer

1. INTRODUCTION

Graph theory has become a foundational tool in network security, offering valuable insights into the structure and dynamics of complex networked systems [1], [2]. Network security involves protecting data and infrastructure from malicious attacks, unauthorized access, and other cyber threats, and graph theory provides a robust mathematical framework for representing and analyzing these systems [3], [4]. By treating networks as collections of nodes connected by edges, graph theory enables researchers to model intricate structures, detect vulnerabilities, and analyze attack vectors [5], [6]. This approach allows for a better understanding of the resilience and weaknesses of networked systems.

One of the key applications of graph theory in network security is in the detection and prevention of cyber-attacks [7], [8]. Graph-theoretic algorithms, such as shortest path, clustering, and centrality measures, are used to identify critical points within networks where attacks are likely to propagate [3], [9]. For instance, centrality measures help in pinpointing influential nodes that, if compromised, could lead to widespread damage. Similarly, clustering algorithms aid in isolating segments within the network, creating more secure and manageable zones that minimize the potential impact of an intrusion [10], [11]. These techniques empower cybersecurity analysts to prioritize security efforts based on the strategic importance of different nodes and paths within the network [12].

Graph theory also enhances anomaly detection, which is crucial in identifying unusual patterns indicative of potential threats [13], [14]. Techniques such as community detection and subgraph analysis allow cybersecurity systems to identify deviations from typical patterns of communication or

[1]Department of Mathematics, Aquinas College, Edakochi, Kochi, Kerala, India
[2]Dept.of Computer Applications, K E College Mannanam, Kerala, India
[3]Department of Mathematics, Little Flower College, Guruvayoor, Kerala, India
[4]Department of Mathematics, Sree Kerala Varma College, Thrissur, Kerala, India
[5]Marian College Kuttikkanam Autonomus, Kerala, India

data flow, which can signal the presence of malicious activities [13], [15]. For example, subgraph isomorphism is used to detect similarities between known attack patterns and new, emerging threats, thereby enabling preemptive responses. Additionally, graph-based machine learning models use historical data to improve threat detection accuracy, offering a proactive stance against evolving cyber threats [16].

The future of network security increasingly relies on the evolving role of graph theory, especially as networks grow in size and complexity with the advent of IoT and cloud technologies [17]. As systems become more interconnected, graph-based approaches are essential for scalable security solutions that can adapt to rapid changes [12]. Current research is exploring new frontiers of graph theory in network security, such as quantum-resistant encryption algorithms and blockchain-based verification, which can further strengthen the integrity and privacy of data [18]. By leveraging the analytical power of graph theory, researchers and practitioners are working toward developing more resilient and adaptive security frameworks, ensuring the robust protection of digital infrastructure [19].

This bibliometric analysis aims to review and synthesize the role of graph theory in network security research, using bibliometric tools such as Biblioshiny and VOSviewer to explore publication trends, influential authors, collaborative networks, and key research themes in this domain [20], [21]. The utilization of Biblioshiny and VOSviewer in this study allows for a comprehensive analysis of the literature, offering insights into the evolution of graph theory applications in network security. Biblioshiny, an R-based application, facilitates data management, citation analysis, and visual representation of bibliometric data [22], [23], [24], while VOSviewer supports the visualization of co-authorship networks, keyword clusters, and thematic evolution over time [25], [26], [27]. By combining the strengths of both tools, this analysis uncovers the patterns and dynamics within scholarly work on graph theory in network security, revealing the key topics, influential works, and emerging areas within the field. This approach not only highlights the existing body of knowledge but also identifies gaps and potential future directions.

This study's findings have implications for both researchers and practitioners in network security, as understanding the literature landscape can guide future research agendas and inform the development of advanced security measures. Insights from graph-theoretic applications in network security are increasingly critical due to the growing complexity of networked systems and the sophistication of cyber threats. As a result, this bibliometric analysis serves as a valuable resource for identifying collaborative opportunities, understanding the current state of research, and charting pathways for innovative solutions that leverage graph theory to enhance network security.

2. MATERIALS AND METHODS

We obtained the scientific publications related to the investigation from the Scopus database [28], [29], [30]. We conducted a search using specific keywords such as "Graph Theory" and "Network Security". The search was not restricted to any particular language, and the data included articles from peer-reviewed journals, book chapters, and conference papers. We collected 961 articles from 573 different sources, spanning 1981 to 2023. To ensure accuracy, we screened the Scopus records to remove any duplicates. The results were saved as a "CSV" file, and we performed bibliometric analysis on the data using VOSviewer and Bibloshiny software.

3. RESULTS AND FINDINGS

3.1. Main Information of the investigation

Table 1 presents the main information investigation, spans from 1981 to 2023, covering 961 documents across 573 sources, with a notable annual growth rate of 12.18%, reflecting a consistent rise in scholarly

attention to this topic. On average, documents are 7.89 years old and receive 20.29 citations, suggesting moderate engagement and influence within the field. The research is characterized by extensive collaboration, as evidenced by an average of 3.34 co-authors per document and 18.42% international co-authorship, while only 65 documents are single-authored, involving 58 authors. The study content is broad, with 6,427 Keywords Plus and 2,491 author keywords, indicating diverse thematic areas. In terms of publication types, conference papers dominate with 530 entries, followed by 425 articles and 6 book chapters, showing that conferences are a primary venue for disseminating research findings in this domain.

Table 1. Main Information of the Investigation

Description	**Results**
MAIN INFORMATION ABOUT DATA	
Timespan	1981:2023
Sources (Journals, Books, etc)	573
Documents	961
Annual Growth Rate %	12.18
Document Average Age	7.89
Average citations per doc	20.29
References	23847
DOCUMENT CONTENTS	
Keywords Plus (ID)	6427
Author's Keywords (DE)	2491
AUTHORS	
Authors	2759
Authors of single-authored docs	58
AUTHORS COLLABORATION	
Single-authored docs	65
Co-Authors per Doc	3.34
International co-authorships %	18.42
DOCUMENT TYPES	
article	425
book chapter	6
conference paper	530

3.2. Annual Scientific Production

Figure 1 presents the annual scientific production of articles on the role of graph theory in network security demonstrates a gradual increase in research output over the years, with significant growth starting around the mid-2000s. Initially, from 1981 to the early 2000s, the publication numbers were sparse, often with only a few articles per year. Notably, from 2006 onwards, there is a clear upward trend, indicating a growing interest and recognition of graph theory's applications in network security. Peaks in productivity are observed in 2009 with 56 articles and a consistent increase each year, reaching a high point in 2023 with 125 articles. This growth trajectory reflects the increasing importance and application of graph theory in addressing modern network security challenges, with research becoming especially active in the last decade. The consistent rise from 2018 onwards suggests a sustained focus in the academic community on this topic, likely due to the rising complexities and demands for robust network security solutions.

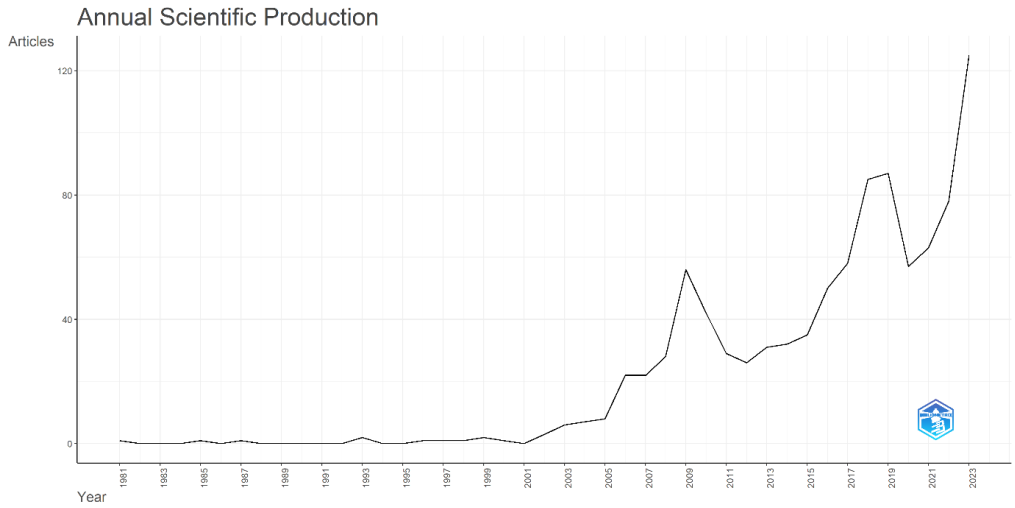

Figure 1. Annual Scientific Production

3.3. Most Relevant Authors

Table 2 presents the most prolific authors in the field of graph theory as applied to network security. Leading the list are Gao, Wei and Hu, Changzhen, each with 7 publications, indicating their substantial contributions and leadership in this domain. Spirakis, Paul follows with 6 articles, demonstrating a strong involvement in the research. Other notable contributors include Chang, Jou-Ming, Mavronicolas, Marios, Papadopoulou, Vicky, Philippou, Anna, Roy, Sandip, Soltan, Saleh, and Srivastava, Anurag, each with 5 articles. This distribution of publications highlights a core group of researchers who have made repeated contributions, reflecting sustained engagement and expertise in exploring the applications of graph theory to enhance network security. Their work likely plays a significant role in advancing knowledge and solutions in this specialized area.

Table 2. Most Relevant Authors

Authors	Articles
GAO, WEI	7
HU, CHANGZHEN	7
SPIRAKIS, PAUL	6
CHANG, JOU-MING	5
MAVRONICOLAS, MARIOS	5
PAPADOPOULOU, VICKY	5
PHILIPPOU, ANNA	5
ROY, SANDIP	5
SOLTAN, SALEH	5
SRIVASTAVA, ANURAG	5

3.4. Most Relevant Sources

Table 3 lists the most relevant sources for publications on the role of graph theory in network security. Lecture Notes in Computer Science (including its subseries) is the leading source with 89 articles, underscoring its prominence as a platform for research in this domain. Following it, the ACM International Conference Proceeding Series and IEEE Access have published 23 and 22 articles,

respectively, reflecting their role in disseminating network security advancements. IEEE Transactions on Smart Grid and Proceedings of SPIE both contributed 9 articles each, highlighting specific applications in smart grids and engineering. Other notable sources include Advances in Intelligent Systems and Computing and Computers and Security, each with 8 articles, as well as Communications in Computer and Information Science, IEEE Transactions on Dependable and Secure Computing, and Reliability Engineering and System Safety, each publishing 7 articles. This distribution illustrates that a diverse range of publications, from general computer science to specialized security and engineering journals, are contributing to the body of knowledge in this field.

Table 3. Most Relevant Sources

Sources	**Articles**
LECTURE NOTES IN COMPUTER SCIENCE (INCLUDING SUBSERIES LECTURE NOTES IN ARTIFICIAL INTELLIGENCE AND LECTURE NOTES IN BIOINFORMATICS)	89
ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES	23
IEEE ACCESS	22
IEEE TRANSACTIONS ON SMART GRID	9
PROCEEDINGS OF SPIE - THE INTERNATIONAL SOCIETY FOR OPTICAL ENGINEERING	9
ADVANCES IN INTELLIGENT SYSTEMS AND COMPUTING	8
COMPUTERS AND SECURITY	8
COMMUNICATIONS IN COMPUTER AND INFORMATION SCIENCE	7
IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING	7
RELIABILITY ENGINEERING AND SYSTEM SAFETY	7

3.5. Most Global Cited Documents

Table 6 lists the most globally cited documents related to graph theory in network security, highlighting key publications based on total citations, citations per year, and normalized citation impact. The most cited paper is by Pasqualetti et al. (2013), published in IEEE Transactions on Automatic Control, with 1,711 total citations and a high citation rate of 142.58 per year, giving it a normalized citation score of 23.50, indicating significant influence. Phillips (1998) and Kosut (2011) follow with 667 and 666 total citations, respectively, with Kosut's paper showing a stronger recent impact with 47.57 citations per year and a normalized score of 17.03. Other notable papers include Huang (2019) in IEEE Transactions on Industrial Informatics, which has a high recent citation rate of 75.67 per year and the highest normalized impact (25.25), showing rapid influence despite its recent publication. Publications by Ou (2006), Hug (2012), Sheyner (2002), Theodorakopoulos (2006), Johansson (2010), and Ingols (2006) also feature prominently, each contributing valuable insights and frameworks to the network security field, evidenced by their consistent citation rates and contributions to foundational knowledge in the area.

Table 4. Most Globally Cited Documents

Paper	DOI	Total Citations	TC per Year	Normalized TC
PASQUALETTI F, 2013, IEEE TRANS AUTOM CONTROL	10.1109/TAC.2013.2266831	1711	142.58	23.50
PHILLIPS C, 1998, PROC NEW SECUR PARADIGMS WORKSHOP	10.1145/310889.310919	667	24.70	1.00
KOSUT O, 2011, IEEE TRANS SMART GRID	10.1109/TSG.2011.2163807	666	47.57	17.03
OU X, 2006, PROC ACM CONF COMPUTER COMMUN SECUR	10.1145/1180405.1180446	529	27.84	6.56
HUG G, 2012, IEEE TRANS SMART GRID	10.1109/TSG.2012.2195338	485	37.31	9.62
HUANG J, 2019, IEEE TRANS IND INF	10.1109/TII.2019.2903342	454	75.67	25.25
SHEYNER O, 2002, PROC IEEE COMPUT SOC SYMP RES SECUR PRIVACY	10.1109/SECPRI.2002.1004377	445	19.35	2.36
THEODORAKOPOULOS G, 2006, IEEE J SEL AREAS COMMUN	10.1109/JSAC.2005.861390	436	22.95	5.41
JOHANSSON J, 2010, RELIAB ENG SYST SAF	10.1016/j.ress.2010.06.010	348	23.20	9.98
INGOLS K, 2006, PROC ANNU COMPUT SECUR APPL CONF ACSAC	10.1109/ACSAC.2006.39	335	17.63	4.15

3.6. Trend Topics

Figure 2 illustrates the trend topics in research related to graph theory and network security over time. Each term represents a key research focus, with the size of the circles indicating term frequency, reflecting its popularity in the literature. Starting from the early 2000s, foundational topics such as "network security," "cyber security," "fault tolerance," "privacy," and "algorithms" were prominent. In recent years, more specialized topics have gained traction, including "cyber-physical systems," "adversarial attack," "machine learning," "threat modeling," and "graph neural networks." These emerging topics indicate a shift towards addressing modern challenges, such as securing interconnected systems, combating adversarial threats, and integrating AI-driven techniques like graph neural networks for enhanced security. The increasing frequency of these terms suggests a growing focus on advanced methodologies to address the evolving complexities in network security. This trend reflects how research priorities in network security are adapting to the latest technological advancements and threat landscapes.

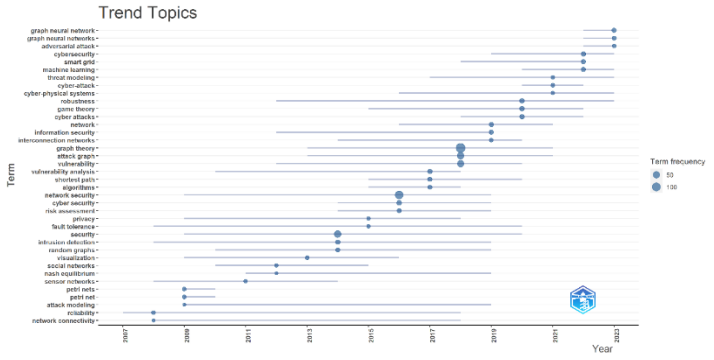

Figure 2. Trending topics in role of graph theory in network security

3.7. Thematic Map

The thematic map categorizes topics in graph theory and network security research into four quadrants based on their development (density) and relevance (centrality). Motor Themes (Top-Right Quadrant): These are well-developed and central themes critical to the field. Topics here, such as "anomaly detection," "machine learning," and "cloud computing," represent active areas of research with strong connections to other topics, indicating their importance and rapid development. These themes are at the forefront of integrating advanced technologies into network security. Niche Themes (Top-Left Quadrant): These topics, like "cryptography" and "intrusion detection system," are specialized, highly developed but less central, meaning they are advanced in their specific scope but may have fewer connections to broader research areas. These themes are crucial in specialized applications within network security but do not directly integrate with other central themes. Basic Themes (Bottom-Right Quadrant): These are foundational and central themes with high relevance but lower development, such as "network security," "attack graph," "cybersecurity," "vulnerability," and "wireless sensor networks." These topics serve as the backbone of research in graph theory and network security, forming the basis for more advanced studies and applications. Emerging or Declining Themes (Bottom-Left Quadrant): These themes, including "social network analysis," "IoT," "graph partitioning," and "network vulnerability," have low development and centrality, suggesting they may either be in the early stages of research or losing traction in this field. Themes in this quadrant may represent nascent areas with potential for growth or fields that are becoming less relevant in the current research landscape. Overall, the thematic map highlights that foundational topics like network security remain essential, while advanced areas like anomaly detection and machine learning are gaining prominence as motor themes in addressing modern security challenges.

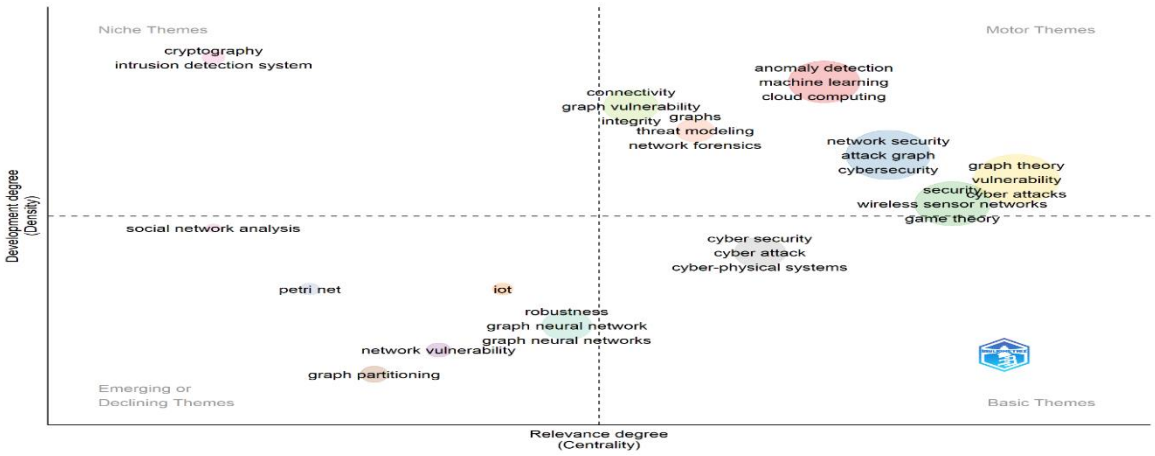

Figure 3. Thematic visualisation of keywords

3.8. Bibliographic Coupling of Sources

Figure 4 presents a bibliographic coupling network of sources, with a minimum citation threshold of 5, highlighting active scholarly discourse in social media banking. The network consists of 19 items organized into 7 clusters, illustrating the relationships between frequently cited sources and identifying major areas of research interest within this domain. Key sources like Lecture Notes in Computer Science and IEEE Access are prominent within the network, indicating their central role in the literature on social media banking and their strong connections with other sources. Lecture Notes in Computer Science appears as a central node with multiple connections across clusters, reflecting its significant impact and broad influence. Other important sources include ACM International Conference Proceedings and IEEE Transactions on Smart Grid, which are highly interconnected, suggesting that research on social media banking often intersects with topics in computer science, smart grid technology, and network security. The color coding of clusters, which ranges from 2014 to 2020, indicates the timeline and development of topics in this field. The sources connected with yellow and green hues are more recent, while those in blue are older, showing the evolution of scholarly focus over time. Emerging topics, shown in recent colors like yellow and green, indicate that newer sources are expanding on areas such as IoT, cybersecurity, and data science as they apply to social media banking. Overall, the network reveals that research in social media banking is highly multidisciplinary, drawing insights from computer science, cybersecurity, and data systems. This interconnectedness suggests a robust exchange of ideas across these fields, with foundational journals and conference proceedings shaping and sustaining the discourse in this evolving area.

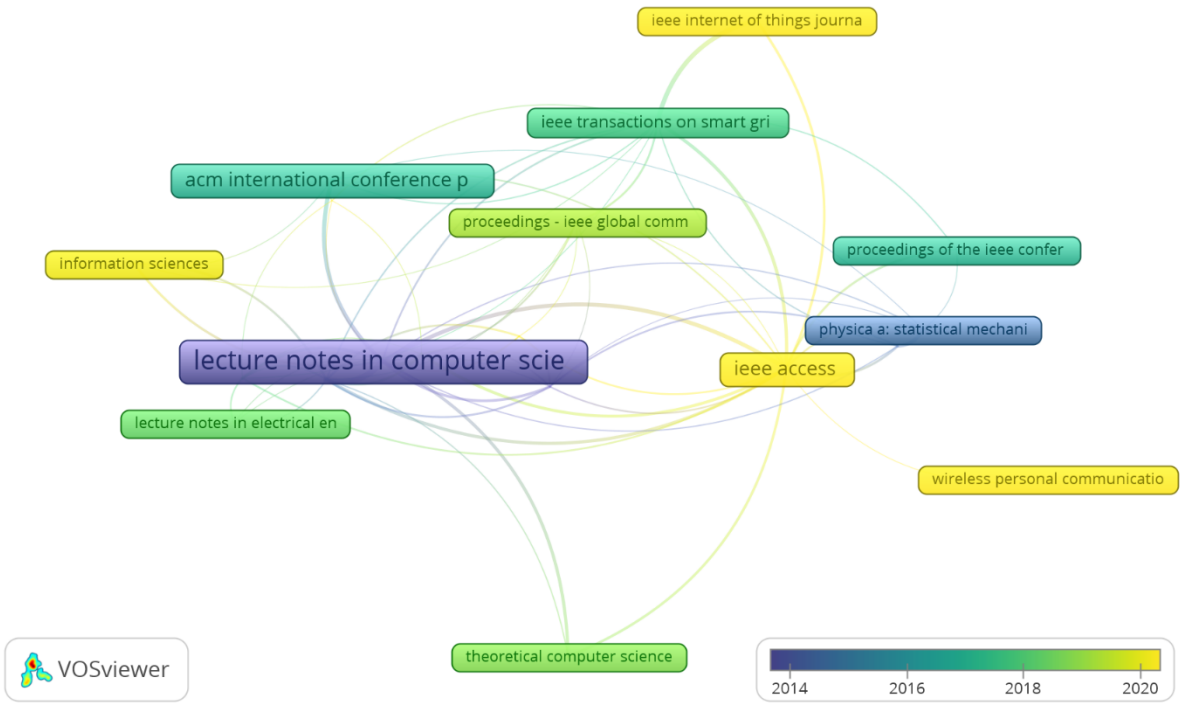

Figure 4. Bibliographic coupling of sources

3.9. Co-occurrence of Keywords

Figure 5 illustrates a co-occurrence network of keywords related to graph theory and network security, with a minimum occurrence threshold of 10. Out of 7,550 keywords, 186 met this threshold, resulting in a network of 66 items categorized into 7 clusters, each represented by different colors and varying in

size based on their frequency and interconnectedness. At the center of the network, "graph theory" emerges as the most prominent keyword, closely linked with foundational topics like security, graph algorithms, and computation theory. This central positioning indicates that graph theory serves as a fundamental framework for various interconnected research areas within network security.

Each cluster represents distinct thematic areas. The Red Cluster (Security and Data Protection) includes keywords like cryptography, security protocols, and mathematical models, focusing on securing information through theoretical and mathematical approaches. The Green Cluster (Detection and Defense Mechanisms), with keywords such as anomaly detection, intrusion detection, and malware, emphasizes identifying and defending against security threats within networks. The Blue Cluster (Optimization and Reliability), featuring terms like optimization, connectivity, and fault tolerance, focuses on enhancing network resilience and efficiency. The Purple Cluster (Infrastructure Security) includes keywords like cyber-attacks, power grids, and smart grids, highlighting the importance of securing critical infrastructure. The Yellow Cluster (Emerging Technologies), with terms like wireless networks and sensor nodes, reflects research on IoT and wireless network security. The Light Blue Cluster (Theoretical and Structural Aspects) includes keywords like shortest path and graph structures, representing the underlying theoretical aspects of graph theory. Finally, the Pink Cluster (Network Modeling and Analysis), with keywords like data mining and feature extraction, is related to analytical techniques for monitoring and assessing network security.

The interconnected lines between keywords in different clusters illustrate the multidisciplinary nature of this research area, where concepts from cryptography, optimization, and critical infrastructure protection intersect. This co-occurrence network highlights the comprehensive application of graph theory across diverse facets of network security, demonstrating the field's evolution to address various contemporary security challenges in complex and interconnected systems. Through these clusters, the network reveals a broad and integrative approach to network security, with graph theory providing a versatile foundation that enables innovation and advancement in addressing current and emerging threats.

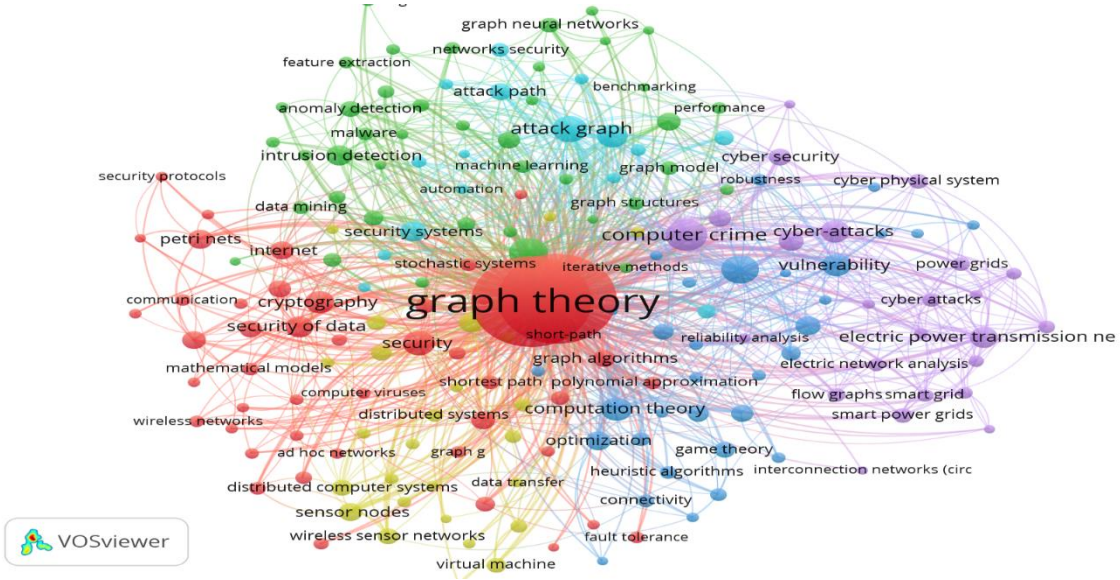

Figure 5. Co-occurrence of all keywords

3.10. Co-authorship of Countries Collaborations

Figure 6 illustrates the co-authorship network of country collaborations in research related to graph theory and network security, based on a minimum document threshold of 5. Out of 79 countries, 33 met this threshold, resulting in a network with 33 items organized into 8 color-coded clusters. Each cluster represents groups of countries that frequently collaborate, with the size of each node indicating the level of publication output and collaboration frequency. China appears as the largest and most central node, indicating its dominant role in this research domain and extensive collaborations with various countries. It is directly connected to countries like Hong Kong, Pakistan, and Iran in its cluster (orange), as well as to other major research hubs in different clusters, reflecting China's broad network of international collaborations. Other prominent clusters include the United Kingdom and Australia (red cluster), showing strong intra-cluster collaboration and connections with countries like Ireland and Finland. In the blue cluster, India collaborates closely with Germany, France, and Switzerland, reflecting a European-Asian research partnership in this field. The diversity in collaboration is further highlighted by clusters such as the green cluster involving Canada, Sweden, and Norway, and the purple cluster with Italy and Greece, which likely indicate regional or thematic research focuses. Overall, the network map reveals that countries with high research output, such as China, India, and the United Kingdom, serve as central hubs fostering international research collaborations. The connections between clusters underscore the global nature of research in graph theory and network security, with strong intercontinental partnerships that promote knowledge exchange and innovation across diverse geopolitical contexts.

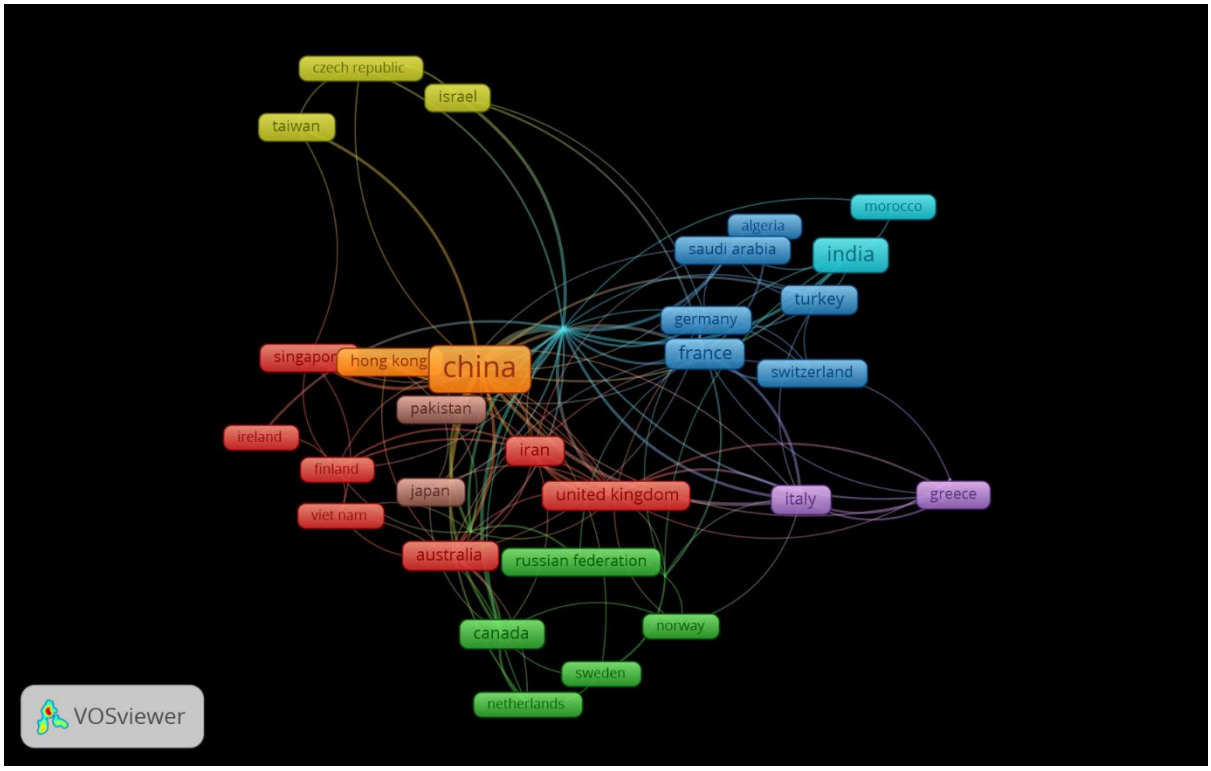

Figure 6. Co-authorship of countries

DISCUSSIONS

The bibliometric analysis of the role of graph theory in network security reveals a steady growth in research output, with a significant increase in publications from 2006 onward. This growth reflects the rising academic interest in utilizing graph theory to address evolving challenges in network security,

driven by the increasing complexity of cyber threats. Leading contributors, such as Gao, Wei, and Hu, Changzhen, have made substantial contributions, highlighting a core group of researchers with repeated publications in the field. This pattern underscores the importance of expert knowledge and sustained research efforts in advancing the understanding and applications of graph theory in network security. Furthermore, prominent sources, including Lecture Notes in Computer Science and IEEE Access, serve as primary platforms for disseminating these research findings, indicating a mix of general computer science and specialized security and engineering journals that contribute to a multidisciplinary body of knowledge.

Analysis of trend topics shows a shift from foundational themes, such as network security and algorithms, to emerging areas like cyber-physical systems, adversarial attacks, and machine learning. This trend highlights the field's adaptation to modern challenges, where securing interconnected systems and combating sophisticated threats require advanced methodologies. The thematic map further categorizes research topics into motor, niche, basic, and emerging themes. Motor themes, like anomaly detection and machine learning, are well-developed and central to the field, suggesting rapid development and integration of these technologies in network security. Meanwhile, basic themes such as cybersecurity and vulnerability analysis serve as the foundation for more advanced studies, while emerging themes like IoT and social network analysis show potential for future growth or shifting relevance.

The co-occurrence network and co-authorship analysis reveal the multidisciplinary and international nature of research in this field. Keywords in clusters represent distinct thematic areas, ranging from security protocols and data protection to optimization and infrastructure security. This network highlights graph theory's comprehensive application across various aspects of network security. Additionally, the co-authorship network shows extensive international collaborations, with countries like China, India, and the United Kingdom acting as central hubs. These collaborations foster knowledge exchange and innovation across diverse geopolitical contexts, underscoring the global response to shared cybersecurity challenges. Together, these findings provide insights into the evolution, key contributors, and collaborative networks in the role of graph theory in network security, offering a roadmap for future research and development in this critical field.

CONCLUSION

This bibliometric analysis highlights the essential role of graph theory in network security, showcasing its capacity to model, detect, and prevent cyber threats effectively. The increasing volume of research and key contributions in this area reflect its importance and rapid evolution to meet modern cybersecurity challenges. Analyzing trend topics and thematic clusters indicates a shift toward integrating advanced techniques, such as machine learning and anomaly detection, to strengthen security frameworks. Moving forward, it is recommended that research expands interdisciplinary applications of graph theory, particularly in emerging fields like IoT and cloud security, to tackle new vulnerabilities in interconnected systems. Additionally, fostering global collaborations remains vital, as international partnerships encourage knowledge sharing and innovation in critical areas like cyber-physical systems. Expanding access to bibliometric tools, such as Biblioshiny and VOSviewer, can further support researchers in tracking developments and identifying research gaps. These efforts collectively aim to enhance the resilience of digital infrastructures against evolving cyber threats.

REFERENCES

[1] N. K. Geetha and V. Ragavi, “Graph Theory Matrix Approach in Cryptography and Network Security,” presented at the Proceedings - 2022 Algorithms, Computing and Mathematics Conference, ACM 2022, 2022, pp. 108–110. doi: 10.1109/ACM57404.2022.00025.

[2] T.-P. Chen, X.-D. Qiao, L.-Q. Zheng, and Y.-Q. Luo, “Application of graph theory in threat situation analysis of network security,” *Beijing Youdian Daxue XuebaoJournal Beijing Univ. Posts Telecommun.*, vol. 32, no. 1, pp. 113–117, 2009.

[3] M. Ming-Zhong, “Network security analysis based on graph theory model with neutral network,” presented at the Lecture Notes in Electrical Engineering, 2012, pp. 551–557. doi: 10.1007/978-3-642-27311-7_73.

[4] T. A. Khaleel and A. A. Al-Shumam, “A study of graph theory applications in IT security,” *Iraqi J. Sci.*, vol. 61, no. 10, pp. 2705–2714, 2020, doi: 10.24996/ijs.2020.61.10.28.

[5] T. Godquin, M. Barbier, C. Gaber, J.-L. Grimault, and J.-M. Le Bars, “Applied graph theory to security: A qualitative placement of security solutions within IoT networks,” *J. Inf. Secur. Appl.*, vol. 55, 2020, doi: 10.1016/j.jisa.2020.102640.

[6] J. Obert and A. Chavez, “Graph Theory and Classifying Security Events in Grid Security Gateways,” presented at the International Journal of Semantic Computing, 2020, pp. 93–105. doi: 10.1142/S1793351X2040005X.

[7] L. Jiang, K. Zhang, J. Xu, and H. Zhang, “A new evidential trust model based on graph theory for open computing systems,” *Jisuanji Yanjiu Yu FazhanComputer Res. Dev.*, vol. 50, no. 5, pp. 921–931, 2013.

[8] P. D. Zegzhda, D. P. Zegzhda, and A. V. Nikolskiy, “Using graph theory for cloud system security modeling,” presented at the Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2012, pp. 309–318. doi: 10.1007/978-3-642-33704-8_26.

[9] N. Li, J. Xia, K. Feng, and R. Liu, “Threat situation analysis of local area network based on the network graph theory model,” presented at the 2009 1st International Conference on Information Science and Engineering, ICISE 2009, 2009, pp. 1927–1930. doi: 10.1109/ICISE.2009.1310.

[10] S. Pirbhulal, V. Gkioulos, and S. Katsikas, “Towards Integration of Security and Safety Measures for Critical Infrastructures Based on Bayesian Networks and Graph Theory: A Systematic Literature Review,” *Signals*, vol. 2, no. 4, pp. 771–802, 2021, doi: 10.3390/signals2040045.

[11] M. K. Sahu, M. Ahirwar, and P. K. Shukla, “Improved malware detection technique using ensemble based classifier and graph theory,” presented at the Proceedings - 2015 IEEE International Conference on Computational Intelligence and Communication Technology, CICT 2015, 2015, pp. 150–154. doi: 10.1109/CICT.2015.147.

[12] G. Rus and A. Brezavšček, “Graph theory applications in computer network security: A literature rewiev,” presented at the Proceedings of the 15th International Symposium on Operational Research, SOR 2019, 2019, pp. 128–134. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085727907&partnerID=40&md5=8eec79299b51bd2e420f4482cf689a2a

[13] L. Song and S. Rho, “Hidden target recognition method for high-speed network security threats based on attack graph theory,” *J. High Speed Netw.*, vol. 29, no. 4, pp. 307–320, 2023, doi: 10.3233/JHS-222048.

[14] M. Jorjani, H. Seifi, and A. Y. Varjani, “A Graph Theory-Based Approach to Detect False Data Injection Attacks in Power System AC State Estimation,” *IEEE Trans. Ind. Inform.*, vol. 17, no. 4, pp. 2465–2475, 2021, doi: 10.1109/TII.2020.2999571.

[15] Z. Wang, M. Zsifkovits, and S. W. Pickl, "Analyzing vulnerabilities of the German high-speed train network using quantitative graph theory," *Int. J. Saf. Secur. Eng.*, vol. 8, no. 1, pp. 59–64, 2018, doi: 10.2495/SAFE-V8-N1-59-64.

[16] C. Zhang, J. Ge, Z. Xia, and H. Du, "Graph Theory Based Cooperative Transmission for Physical-Layer Security in 5G Large-Scale Wireless Relay Networks," *IEEE Access*, vol. 5, pp. 21640–21649, 2017, doi: 10.1109/ACCESS.2017.2761882.

[17] G. Rus and A. Brezavšček, "Graph theory applications in computer network security: A literature rewiev," presented at the Proceedings of the 15th International Symposium on Operational Research, SOR 2019, 2019, pp. 128–134. [Online]. Available: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085727907&partnerID=40&md5=8eec79299b51bd2e420f4482cf689a2a

[18] H. A. Dawood, "Graph theory and cyber security," presented at the Proceedings - 3rd International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2014, 2014, pp. 90–96. doi: 10.1109/ACSAT.2014.23.

[19] M. Lin, Q. Ye, and Y. Ye, "Graph theory based mobile network insight analysis framework," presented at the 2016 IEEE 7th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference, UEMCON 2016, 2016. doi: 10.1109/UEMCON.2016.7777888.

[20] F. Husain and M. S. Mustafa, "A Decade of Islamic Banking Research: Bibliometric Review with Biblioshiny and Vosviewer," *Jambura Sci. Manag.*, vol. 5, no. 2, pp. 67–85, 2023.

[21] D. Kumar, A. K. Shandilya, and S. Choudhuri, "Artificial Intelligence-Enabled Bibliometric Analysis in Tourism and Hospitality Using Biblioshiny and VOSviewer Software," in *AI-Centric Modeling and Analytics*, CRC Press, 2023, pp. 260–291.

[22] M. H. Fahamsyah, I. Mawardi, N. Laila, and M. S. Shabbir, "Global Islamic Banking Development: A Review and Bibliometric Analysis Using R-Biblioshiny Application," *Muqtasid J. Ekon. Dan Perbank. Syariah*, vol. 14, no. 1, pp. 69–92, 2023.

[23] B. D. Ghorbani, "Bibliometrix: Science Mapping Analysis with R Biblioshiny Based on Web of Science in Applied Linguistics," in *A Scientometrics Research Perspective in Applied Linguistics*, H. Meihami and R. Esfandiari, Eds., Cham: Springer Nature Switzerland, 2024, pp. 197–234. doi: 10.1007/978-3-031-51726-6_8.

[24] R. Komperda, "Likert-type survey data analysis with R and RStudio," *ACS Symposium Series*, vol. 1260. pp. 91–116, 2017. doi: 10.1021/bk-2017-1260.ch007.

[25] A. F. Abbas, A. Jusoh, A. Masod, and J. Ali, "A Bibliometric Analysis of Publications on Social Media Influencers Using Vosviewer," *J. Theor. Appl. Inf. Technol.*, vol. 99, no. 23, pp. 5662–5676, 2021.

[26] R. Kumar, S. Saxena, V. Kumar, V. Prabha, R. Kumar, and A. Kukreti, "Service innovation research: a bibliometric analysis using VOSviewer," *Compet. Rev. Int. Bus. J.*, vol. 34, no. 4, pp. 736–760, 2024.

[27] A. Kuzior and M. Sira, "A bibliometric analysis of blockchain technology research using VOSviewer," *Sustainability*, vol. 14, no. 13, p. 8206, 2022.

[28] J. Baas, M. Schotten, A. Plume, G. Côté, and R. Karimi, "Scopus as a curated, high-quality bibliometric data source for academic research in quantitative science studies," *Quant. Sci. Stud.*, vol. 1, no. 1, pp. 377–386, Feb. 2020, doi: 10.1162/qss_a_00019.

[29] Y. Gavel and L. Iselid, "Web of Science and Scopus: a journal title overlap study," *Online Inf. Rev.*, vol. 32, no. 1, pp. 8–21, 2008.

[30] A.-W. Harzing and S. Alakangas, "Google Scholar, Scopus and the Web of Science: a longitudinal and cross-disciplinary comparison," *Scientometrics*, vol. 106, pp. 787–804, 2016.