Online at: https://researchtrendsjournal.com
Indexed Journal

ISSN No: 2584-282X
Peer Reviewed Journal

INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT

Volume 3; Issue 4; 2025; Page No. 447-453

Received: 03-04-2025
Accepted: 12-06-2025
Published: 22-07-2025

Graph Theory and Network Analysis: Emerging Applications in Social Networks, Cybersecurity, And Artificial Intelligence

[1]Madhvi Dhopte and [2]Dr. Akhilesh Kumar Dwivedi

[1]Research Scholar, Mahakaushal University, Jabalpur, Madhya Pradesh, India
[2]Associate Professor, Mahakaushal University, Jabalpur, Madhya Pradesh, India

DOI: https://doi.org/10.5281/zenodo.20674305

Corresponding Author: Madhvi Dhopte

Abstract

Graph theory is a branch of mathematics concerned with the study of graphs, which are mathematical structures that express pairwise connections between things. The fundamental tools for comprehending Graph theory and network analysis are used in this field to give light on the structure and behaviour of social systems. Graph theory is a vital tool for solving theoretical and practical problems due to its capacity to represent and analyze complicated systems.

Keywords: Graph theory, graphic, depiction and mathematics

Introduction

The field devoted to the study of graphs is called theory of graphs. The study of graphs is the focus of this mathematical subject. This graphic depiction represents the mathematical reality. In graph theory, the relationships between nodes (vertices) and lines (edges) are studied.

In discrete mathematics, graph theory refers to the study of graphs. One mathematical representation of a function is a graph, which is just a series of points connected by lines. Its primary function is to link two items together in a paired fashion. The graph's vertices (nodes) are linked together by the does (lines). There are many other fields that make use of the linear graph beyond mathematics, including computer science, chemistry, biology, linguistics, and physics. The greatest real-world example of graph structure is GPS, which lets you follow a route or find the direction of a road.

Computer processing of molecular structures, such as database searching and chemical editing, is a strong suit of this technology. The local interactions between interacting components of a system or the dynamics of a physical process on a system may be shown via graphs in statistical physics.

Graph theory's techniques are effectively used in social network analysis, which focuses on networks and their properties. Graph theory essentially sees social networks as mathematical structures comprised of nodes (individuals) and edges (connections or interactions). This form may be used with a number of graph theoretic concepts and techniques to anticipate behavior in these networks, detect trends, and quantify impact. Connected sets of discrete items called "vertices" make up a graph by lines or edges. Graphs, which depict both independent entities and the connections between them, are used for issue modeling in many domains. A graph is a graphical representation of data that uses points, circles, or nodes to depict things and lines to express the relationships between them (Diestel, 2017) [12].

Graphs, such structures consist of vertex structures (also known as nodes) and edge structures (which link pairs of nodes), are the subject of graph theory, a well-known area of mathematics. Graph theory has grown into an important area with several applications across many fields since its introduction by Leonhard Euler in the 18th century to resolve the famous Königsberg Seven Bridges problem.

These fields include computer science, biology, sociology, and network security, among many others. The difference between directed and undirected graphs is that the former have edges with directions and the latter have not. Weighted graphs can allow for the representation of costs, distances, or capacities along edges. Graphs are able to represent complex systems and interactions in a simple and easily understood way because of their adaptability.

Literature Review

Permata Dewi, Shinta *et al*. (2024) [1]. Social Network Analysis in Graph Theory and Its Programming for social networking platforms. "Graph theory" has its roots in mathematics delves into the web of relationships between nodes and edges. By visualizing people and their connections as graphs, social network analysis is able to model and study social systems. With persons represented as nodes and their interactions (such as friends, followers, or connections) as edges, social media networks like LinkedIn, Facebook, and Twitter provide useful data for this study.

Wang, Shuo. (2025) [2]. Graph theory's use in studying information and social networks is the focus of this literature review. To begin, we define a few essential network parameters, including the clustering coefficient (transitivity), centrality, and diameter, all of which are fundamental to comprehending the dynamics of information diffusion within networks. Following this, we discuss the ways in which these features allow graph theory to be used in the investigation of social and information networks. Our review concludes with a look at several useful social and informational models, including the Linear Threshold and SIR programs.

Golędzinowski, Wojciech *et al*. (2024) [3]. To show how important This article explains how SNA may help you comprehend group dynamics, information flow, social structures, and effect will look at its theoretical underpinnings and practical applications. Data collecting, network visualization, and network metrics are only a few of the approaches and technologies covered in the article that pertain to SNA research. This article invites more investigation into this rich topic by providing a thorough evaluation of SNA methods and their uses, which adds to the expanding body of knowledge in the study of social networks.

Diogo, Vicente. (2024) [4]. Social Networks and Graph Theory: A Quick Overview. Mathematics is the foundational science upon which the rules of the universe are founded, but it is also much more than that. Every aspect of our everyday life relies on arithmetic, from the most basic task of counting coins to the most intricate architectural structures. By delving into the links between Discrete Math and Network Sciences analysis-specifically, graph theory and its use to social networks-this essay investigates the unexpected ways math is entering our daily life.

Katharina Zweig. (2016) [5]. Due to its generalizability, network analysis has been developed and utilized in several fields; it offers a flexible framework for modeling complicated systems. The three most well-known fields in this area are statistical physics, graph theory, and sociology; each of them adds something unique to the subject via its own viewpoint and methods. Given the divergent goals of these fields, familiarity with their respective methods and points of view is essential. This section delves more into the issue at hand by outlining and countering the many techniques to emphasize the most crucial aspects-familiarity with network analysis.

Graph Theory Network Analysis

Theoretical Framework for graphs Mathematics and computer science come together in the field of network analysis, which models linkages and processes in different systems via the study of graphs. It is fundamental for learning about the behavior and structure of networks in many different areas, including:

- **Computer Science:** Enhancing data structures and algorithms.
- **Biology:** Interaction network analysis of proteins.
- **Social Network Analysis:** Comprehending patterns of influence and social dynamics.

In today's data-driven world, this multidisciplinary approach is essential since it improves theoretical understanding and drives breakthroughs in practical applications.

Key Concepts and Terminologies

Graph theory and network analysis rely on a handful of essential concepts:

- **Adjacency Matrices:** A finite graph is represented by a square matrix. The matrix's members show the degree of proximity between two graph vertices.
- **Path:** A group of unconnected edges that connect a collection of nodes.
- **Cycle:** A non-repetitive route is one that begins and terminates at the same vertex.
- **Degree:** The number of edges that meet at a certain vertex. There are two parts to directed graphs: in-degree and out-degree.
- **Connectivity:** This property describes the degree of connectivity between nodes in a graph, including ideas like linked components in undirected graphs and highly linked components in directed graphs.

Graph Algorithms and Their Applications

In network analysis, graph algorithms are crucial. For example, In contrast to Dijkstra's algorithm, which finds the shortest path, Prim's and Kruskal's methods identify the fewest trees that contact each other. Efficiently tackling complicated issues is made possible by these algorithms and many more. For example, routing and navigation systems rely heavily on Dijkstra's algorithm to determine the fastest way.

In order to keep wire costs low and connection high, networks such as telecommunication systems often use Prim's and Kruskal's algorithms during design.

Among the various graph algorithms available in Tom Sawyer Perspectives, a platform for developing applications that visualize and analyze graphs with no code, are some that help find out which nodes and edges are most important. To resolve problems in digital engineering, supply chain management, social network analysis, digital transformation, digital engineering, path, centrality, network flow, and tree analysis, Perspectives offers methods for traversal, clustering, partitioning, path, cycle, and network flow.

The importance of these graph algorithms in optimizing and addressing network flow issues across many areas is highlighted by their applications, which are crucial for extracting value and intelligence from data.

Tools and Technologies for Graph Theory Network Analysis

When dealing with networks of varying sizes and complexity, graph theory network analysis has become an essential tool in many fields. In addition to analytical methods, Perspectives has powerful graph visualization features, making it ideal for this purpose.

Graph theory network analysis relies heavily on visualization as complicated networks are intrinsically hard to understand when presented with only numerical data. By using visualization, one may have a better understanding of the network's architecture, spot trends, and spot unusual occurrences. Visualization tools like Tom Sawyer Software Perspectives make it easy to examine community structures, node centrality, and network density, among other network aspects. By simplifying and enhancing the visual representation of data, effective visualization aids in disseminating results to a wider audience.

Researchers are able to derive insights from the visual depiction of data using visualization methods, which aids in both hypothesis formulation and testing. New hypotheses on the dynamics and behavior of a network may be developed by visualizing its connections and flows. Because the visual depiction of networks may unite seemingly disparate areas of study, this is an essential component of multidisciplinary research.

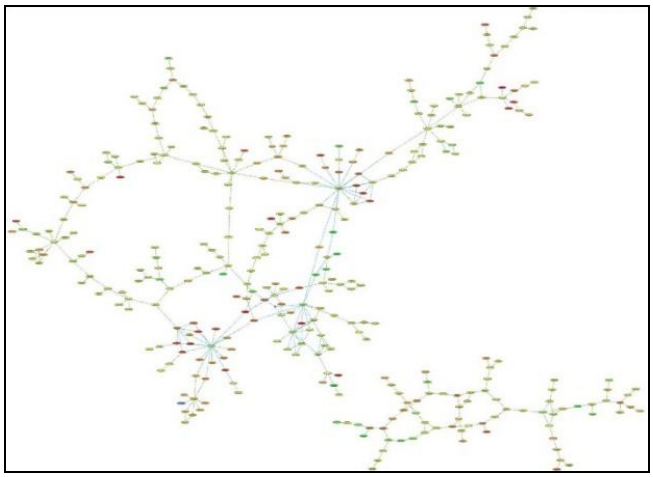

Fig 1: Graph Theory Network Analysis

An extensive visual representation of a network's topology created using Tom Sawyer Software Perspectives.

Computational Challenges in Large-Scale Networks

It is computationally challenging to analyze large-scale networks like the Internet, transportation systems, or social networks. The amount of time and memory needed by algorithms for network analysis might grow exponentially due to the large number of nodes and edges. To study such massive networks, you may rely on Perspectives fine-tuned and scalable algorithms.

Further complicating matters is the fact that nodes and edges in real-world networks often have dynamic characteristics, meaning they arise and vanish over time. To overcome these obstacles, efficient data structures must be developed. Distributed systems and parallel computing provide potential answers by making better use of several processors to process massive datasets.

Integration of Artificial intelligence and ML

Graph theory, network analysis, AI, and ML all working together, provide an exciting new avenue for research. Learning from the structure and behavior of networks to forecast future connections is one example of how AI and ML may improve network analysis. Other ways in which AI and ML can improve network analysis include predicting how networks will evolve and identifying patterns or abnormalities.

Looking Ahead to Graph Theory and Network Analysis: Where Do We Go from Here?

The next big thing is going to shake up a few fields, including graph theory and network analysis:

- **Quantum Computing:** Because quantum computers can do calculations at rates that conventional computers can't match, they might completely alter the landscape of network research. The time needed to analyze large-scale networks might be drastically cut down if this happens.
- **Network Science as a Service:** Network research as a service might be on the horizon, thanks to the proliferation of cloud computing and as-a-service models. This would open up computing resources and sophisticated network analysis tools to more people, encouraging innovation in many different fields.
- **Interdisciplinary Approaches:** Intersections between network analysis and fields like physics, sociology, and biology are only going to become deeper. New understandings of the underlying principles controlling complex systems may be revealed via this multidisciplinary approach.
- **Ethical and Privacy Considerations:** Ethical and privacy concerns will inevitably take center stage as the use of personal data in network research grows, particularly in social networks. The development of privacy-preserving frameworks for ethical network analysis is of the utmost importance.

Ethical Considerations in Network Analysis

Ethical concerns are becoming more prominent in the field of network analysis as our capacity to gather, process, and understand massive volumes of data from networks (including transportation systems and social media interactions) grows. Issues with privacy, security, and the moral application of network analysis rank high on this list. Taking these factors into account is important for several reasons, including staying in compliance with the law, building trust, and making sure technology is used responsibly.

Privacy

Data gathering and utilization are at the heart of privacy issues in network research. Protecting networks from unwanted access and exploitation is crucial because they

often hold personal information about people's habits, likes, and social connections. It is essential to get informed permission from persons whose data is studied, adhere to data minimization rules, and be transparent about data gathering techniques in order to do network analysis ethically. Furthermore, in order to safeguard people' identities while maintaining the validity of the study, pseudonymization and anonymization procedures should be used.

Security

Privacy issues are inextricably bound up with the safety of data sent via networks. Cybercriminals target data repositories that store and handle massive datasets since network analysis is a data-intensive field. Encryption, access limits, and routine security audits are all part of a comprehensive cybersecurity strategy for protecting network data. These safeguards aid in avoiding data breaches that can jeopardize people's privacy by exposing sensitive information.

Ethical Use

Considerations of justice, responsibility, and non-discrimination are part of the ethical use of network analysis that goes beyond privacy and security. Unfair or biased results may result from network analysis if it reinforces preexisting biases in the data. Recognizing and reducing these kinds of biases is an important part of doing ethical network analysis. To avoid unintentionally hurting certain groups or people, A thorough analysis of the data, methods, and results interpretation is required. Also, if network analysis has any unintended consequences, there has to be a system in place to hold people accountable.

The Application for Graph Theory in Intrusion Prevention Systems

Numerous areas of the powerful resources and mechanisms for network security models offered by graph theory, the mathematical study of graphs. Network topology analysis, intrusion detection systems, attack graphs, access control, security analytics using graph databases, malware propagation, social network analysis, cryptographic networks, and cryptographic networks are a some of the significant applications of graph theory to the field of network security that are examined in this research.

Network Topology Analysis

By visualizing the network's components as graphs, one may get understanding of the setup and topology of the network. The nodes (vertices) in this network diagram stand for the equipment, such as computers, routers, and switches, and the communication lines between them are shown as edges. The network's architecture, any weaknesses, and design optimization for increased security and performance may be better understood and addressed with the help of this visual depiction.

Graph Representation: A variety of graphs are useful for depicting network architecture, including:

1. **Undirected Graphs:** In cases when the edges do not indicate a direction, they stand for connections that may go both ways.
2. **Directed Graphs:** The direction of data flow is indicated by edges that have a direction.
3. **Weighted Graphs**: In cases where edges have weights-for example, latency or bandwidth-that reveal the link's capability or cost.

A network's structure and behavior may be better understood with the help of several types of graphs

- **Vulnerability Identification:** Finding weak spots in a network is a major advantage of doing a topology study. In order to comprehend and strengthen the network, many graph-theoretic metrics are used.
- The degree of centrality is defined as the number of edges connecting a node. Considering that an agreement to a very central node might have far-reaching consequences for the network, these nodes are considered essential. An example of a high-degree node whose failure might interrupt network communication is a router with numerous connections.
- **Closeness Centrality:** Specifies the rate at which data may propagate over the whole graph. For effective communication, nodes having a high proximity centrality are vital. Data transmission reliability and speed might be impacted if these nodes were hacked.
- **Betweenness Centrality:** Finds nodes that connect various sections of the network. Data flow relies on these nodes since they are positioned on the paths that connect other nodes the quickest. To thwart assailants from eavesdropping or interfering with communication, it is crucial to secure these nodes.
- **Resilience and Fault Tolerance:** Analyzing a network's robustness and fault tolerance is another use of graph theory. The graph of the network can tell security experts how resistant it is to assaults and failures. As an example, think about:
- **Connectivity:** The extent to which the network maintains connectivity in the event of failures at nodes or edges. If the network is highly connected, it means it can handle many failures without breaking apart.
- **Redundancy:** Having more than one route connecting nodes. The network's stability is enhanced by having redundant pathways, which allow for the use of an alternate path in the event that one path fails.

Optimal Network Design: Graph theory allows for the development of optimum network architectures that guarantee safe and efficient communication. Procedures like:

- **Minimum Spanning Tree (MST):** Reduces complexity and costs by assisting in the design of networks with few edges that nonetheless retain connection.
- The Max Flow-Min Cut Theorem determines the highest possible data flow via a network and any bottlenecks, then uses that information to direct improvements that boost capacity and performance.

Intrusion Detection Systems (IDS)

Anomaly Detection: By representing typical network activity as a graph, graph theory provides a strong foundation for intrusion detection systems. Entities (such as people or devices) are represented by nodes in this

paradigm, while interactions or communications are represented by edges. It is possible to detect suspicious activity, such as an intrusion, if this predefined network structure deviates in any way from it. An indication of malicious behavior might be a rapid increase in communication between two nodes that normally do not engage with one other.

Graph-based Algorithms: Inconsistent patterns in network traffic may be detected using a number of graph-based methods. Unusual data routing may be detected by shortest route algorithms, aberrant group behavior by clustering algorithms, and nodes that have grown central owing to greater interactions can be located by centrality measurements; all of these things might hint to a security risk.

Attack Graphs

Attack Paths: Attack graphs represent possible entry points that a hacker may use to breach a network. Nodes in these graphs stand for network states, while edges between them indicate exploit-induced state shifts. For the purpose of network security, this lets experts see and evaluate every potential route an attacker may take to reach a certain target.

Risk Assessment: Because they show the probability and effect of various assault scenarios, attack graphs are a priceless tool for risk assessment. Security teams may better prioritize defenses and spend resources to reduce the most significant risks if they have a good grasp of these possible attack vectors. By taking this preventative measure, we can improve the network's defenses.

Access Control, Fourth Edition

Controlling Access Based on Roles (RBAC): Graph theory is crucial for optimizing and modelling access control procedures. This graphic shows the relationship between roles and users on the one hand, and permissions on the other, using a bipartite graph the relationship between roles, users, and RBAC systems. The assignment of roles and permissions to those roles are represented by edges. The proper management of access privileges and the minimization of disputes are guaranteed by this visual depiction.

Policy Verification: Access control rules may also be verified using graph-based methods. Security teams may see the graph and check for conflicts or accidental permissions to access. This check ensures that critical resources cannot be accessed by unauthorized parties and helps keep the access control system secure.

Network Flow Analysis

Flow Networks: By drawing a flow graph of the network, graph theory helps in studying and improving the network's flows. In this graph, the nodes represent individual nodes in the network, while the edges show the bandwidth or data flow capacity. Flow networks are useful for figuring out where optimization is required and for comprehending data flow via the network.

Bottleneck Identification: Security experts may learn a lot about how to make networks more secure and efficient by analyzing flow networks. When data becomes too congested at a bottleneck, the network becomes susceptible to attacks like denial of service (DoS). The efficiency and safety of network operations may be enhanced by locating and eliminating these obstacles.

Malware Propagation

Epidemic Models: Epidemic models on graphs allow one to study the propagation of malware inside a network. To better comprehend the malware's propagation via the network, models like the Susceptible-Infected-Recovered (SIR) model are useful. Edges stand for possible vectors that malware might use to propagate from one device to another, whereas nodes stand for devices themselves.

Containment Strategies: Graph theory is useful for figuring out how to stop or limit the spread of malware. It is possible to interrupt the spreading of malware by implementing targeted interventions after identifying key nodes or edges that are involved. For instance, if you want to successfully confine the infection, you may disconnect or strengthen the protection surrounding these vital locations.

Social Network Analysis

User Behavior: When it comes to social network analysis, graph theory may be a lifesaver when trying to spot suspicious activity. In a social network graph, users are shown as nodes, and the relationships between them are shown as edges are represented by edges. Malicious group development, strange communication patterns, and the proliferation of phishing attempts are just a few examples of the patterns that may be uncovered by analyzing this graph.

Influence and Trust: According to graph theory, centrality metrics reveal which nodes or users have a disproportionate amount of sway in a network. Cybercriminals may specifically target these people in an effort to disseminate false information or harmful files. To better monitor and mitigate such risks, it is helpful to understand the network's impact and trust connections.

Cryptographic Networks

Secure Communication: Cryptographic protocols, which guarantee safe communication inside a network, are designed and analyzed using graph theory. For instance, graph-theoretic methods may be used to optimize key distribution, making ensuring that keys are disseminated safely and effectively across nodes in the network. This improves the communication's security by reducing the likelihood of key compromise.

Network Coding: To make data transfer via networks more secure and efficient, graph-based methods are used. The goal of network coding is to increase data flow while decreasing the likelihood of data interception or manipulation by mixing data from several sources. Data transfer is guaranteed to be safe and dependable using this method.

Challenges In Network Analysis Using Graph Theory

Graph theory has many useful applications, but there are

several obstacles to overcome when using it to network research:

1. **Computational Complexity:** Computational needs for large-scale network analysis tend to be high since the number of nodes and edges involved grows exponentially.
2. **Dynamic Behavior of Networks:** Creating effective techniques for dynamic analysis is a continuous problem real-world networks are dynamic because nodes are always being added or removed.
3. **Data Privacy Concerns:** Ethical concerns about privacy must be thoroughly addressed throughout analytic procedures in networking research due to the growing involvement of personal data, particularly in social networks.
4. **Integration with Emerging Technologies:** While there are many potential benefits of combining AI and ML with more conventional graph-based methods, there are also some drawbacks, such as issues with algorithmic bias and interpretability.

Graph Databases for Security Analytics

Data points with complicated links and interconnections may be handled by specialized storage and management systems called graph databases. Graph databases utilize an adaptable, schema-less paradigm that depicts data as entities represented as nodes and connections between them, as opposed to the rigid tables and predetermined schemas used by conventional relational databases. Given the importance of comprehending and traversing complex links in security analytics, graph databases are naturally well-suited for the job.

Representing Security Data

- Common types of data used in security analytics include system statuses, network traffic, user actions, warnings, and events. Graph databases are great at representing this kind of data:
- Nodes are able to stand in for a wide range of things, including people, gadgets, internet protocol addresses, data, and programs.
- Edges possible to indicate connections or exchanges between various things, including credentials, data transfers, and authorization to access resources.

With this setup, security data may be dynamically and comprehensively represented, allowing for the capture of the complex web of interactions prevalent in an IT setting.

Advantages of Graph Databases in Security Analytics

- **Enhanced Detection of Complex Threats:** When it comes to finding intricate, multi-stage assault patterns, graph databases really shine. Security analysts may find coordinated assaults by following the graph's edges. As an example, a malicious actor might extend their privileges and traverse the network laterally by using a compromised account. Graph databases are able to follow these phases, which unveils the route of the assault.
- **Real-time Analysis and Visualization:** Graph databases provide real-time updates and queries due to its schema-less design. By ingesting security events and instantly associating them with existing data, real-time detection and reaction are made possible. By combining visualization tools with graph databases, analysts may get a better understanding of security occurrences via understandable graphical representations. This facilitates their investigation into potential dangers.
- **Correlation and Contextualization:** Security occurrences tend to happen one after another, which makes it hard to figure out what they mean. Through the use of connections, graph databases are able to correlate seemingly unrelated occurrences. For instance, it may be indicative of a possible brute-force assault if the same IP address repeatedly tries to log in but is unsuccessful before finally succeeding. Precise threat identification and response rely on this contextualization.
- **Scalability and Flexibility:** These days, graph databases can easily manage massive amounts of data because to their horizontal scalability. No complicated schema changes are required for graph databases to grow in size as security data increases. Because of this adaptability, the database may adapt to the changing security requirements of the enterprise without sacrificing performance or relevance.

Use Cases in Security Analytics

- **Intrusion Detection and Response:** Anomalies may be detected by graph databases by finding departures from predicted patterns, which they use to represent typical network activity. As an example, suspicious activity may be indicated by non-standard communication between normally inactive nodes.
- **Identity and Access Management:** Anomalies may be detected by graph databases by finding departures from predicted patterns, which they use to represent typical network activity. As an example, suspicious activity may be indicated by non-standard communication between normally inactive nodes.
- **Threat Intelligence and Hunting:** By connecting threat intelligence data with internal security records, graph databases may be used by security analysts. In order to swiftly detect and evaluate such dangers, analysts may map recognized indicators of compromise (IOCs) to internal activities.

Compliance and Auditing: Because they show user actions and access patterns clearly, graph databases make it easier to monitor whether or not security standards are being followed. The auditing process and compliance with regulatory standards are both aided by this openness.

Conclusion

There is a vast array of fields and applications that can benefit greatly from social network analytics that make use of graph theory. These include healthcare, business intelligence, marketing, churn prediction, online communication analysis, links, telecoms, and the financial sector, and many more. The importance processing graphs systems is growing as the number of issues using graphs increases. We were able to learn more about the unique

characteristics of each graph processing system by comparing the three systems with data sets that varied in size and characteristics.

References

1. Permata Dewi S, Prihandini R, Jannah D, Makhfudloh II, Agatha A, Wulandari Y. Social network analysis in graph theory and its application to social media platforms. 2024.
2. Wang S. Application of graph theory in social network analysis. Theoretical and Natural Science. 2025;79:173-179. doi:10.54254/2753-8818/2025.20135.
3. Golędzinowski W, Błocki W. Social network analysis: From graph theory to applications. Social Communication. 2024;24:151-164. doi:10.57656/sc-2023-0012.
4. Diogo V. A glimpse on graph theory and social networks. 2024.
5. Zweig KA. Graph theory, social network analysis, and network science. In: Network Analysis Literacy: A Practical Approach to the Analysis of Networks. Vienna: Springer; 2016. doi:10.1007/978-3-7091-0741-6_2.
6. Devineni S, Gorantla B. Graph theory and algorithms for social network analysis. Computer Science Engineering and Technology. 2024;3:52-60. doi:10.46632/jdaai/3/1/7.
7. Kolomeets M, Chechulin A, Kotenko I. Social networks analysis by graph algorithms on the example of the VKontakte social network. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications. 2019;10:55-75. doi:10.22667/JOWUA.2019.06.30.055.
8. Phule S. Applications of graph theory in networking and social media. International Journal of Advanced Research in Science, Communication and Technology. 2024:466-472. doi:10.48175/IJARSCT-15778.
9. Tripathi A, Gaur A, Sri S. Implementation and analysis of social network graph in interpersonal network. Jurnal Ilmu Komputer. 2020;13:5. doi:10.24843/JIK.2020.v13.i02.p03.
10. Tabassum S, Pereira FSF, Fernandes S, Gama J. Social network analysis: An overview. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2018;8:e1256. doi:10.1002/widm.1256.
11. Alamsyah A, Rahardjo B, Kuspriyanto. Social network analysis taxonomy based on graph representation. arXiv [Preprint]. 2021. doi:10.48550/arXiv.2102.08888.
12. Liu W, Sidhu A, Beacom A, Valente TW. Social network theory. In: The International Encyclopedia of Media Effects. Hoboken (NJ): John Wiley & Sons; 2017. doi:10.1002/9781118783764.wbieme0092.
13. Akhtar N, Ahamad M. Graph tools for social network analysis. In: Research Anthology on Social Network Analysis and Mining. Hershey (PA): IGI Global; c2021. p. 511-530. doi:10.4018/978-1-7998-7297-9.ch025.
14. Barman K, Patra K. Exploring the structure of social media network with the concepts of graph theory. International Journal of Engineering and Advanced Technology. 2020;9:1136-1141. doi:10.35940/IJEAT.D8306.049420.
15. Chakraborty A, Dutta T, Mondal S, Nath A. Application of graph theory in social media. International Journal of Computer Sciences and Engineering. 2018;6:722-729. doi:10.26438/ijcse/v6i10.722729.