Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 8, pp. 3051–3064
DOI : 10.47974/JDMSC-2690

Enhancing network security with graph theory through identification of critical nodes and vulnerabilities

Y. M. Manjunath [†]
H. L. Parashivamurthy *
Department of Mathematics
BGS Institute Technology
Adichunchanagiri University
B. G Nagara
Mandya 571811
Karnataka
India

S. Girish Babu [§]
G. Manjunath [‡]
Department of Mathematics
R R Institute of Technology
Bangalore 560090
Karnataka
India

Abstract

The concept of network security is on the increase in the digital era and cyber threats have increasingly become more advanced and sophisticated. This study examines the research of finding critical nodes with the help of a graph theory and determining weaknesses in network structures. The analysis of the network based on centrality metrics which include degree, betweenness and closeness centrality names important node identities that are essential in ensuring the network remains connected and efficient. The effect of node failure is estimated using the MATLAB simulation, and it is concentrated on how the centrality of nodes is compromised to cause network fragmentation and performance deterioration. The findings demonstrate the importance of centrality metrics in identifying vulnerabilities in a network, and degree-centrality nodes are the most susceptible systems to failure. Betweenness and closeness centrality also underscore how important nodes are

[†] *E-mail:* **y.manjunath@jaincollege.ac.in**
* *E-mail:* **parashivamurthyhl@bgsit.ac.in (Corresponding Author)**
[§] *E-mail:* **girishbabu.s@rrit.ac.in**
[‡] *E-mail:* **manjunath.g@rrit.ac.in**

in regulating the movement of the network and removing delays. The results confirm the usefulness of the graph theory-related approaches to enhancing the security of the network through providing information on the identification of the key nodes and simulation of attacks. The paper also shows the capabilities of dynamic simulations versus the static methodology that offers real-time analysis of network vulnerabilities and security policies. It is a work in progress to expand these methods to larger networks (including real-time data to detect vulnerabilities) and improve recovery measures in the future.

Subject Classification: *68M25, 18M35, 05C10, 05C30, 05C72.*

Keywords: *Network security, Graph theory, Centrality measures, Vulnerability analysis, MATLAB, Critical nodes, Betweenness centrality, Degree centrality, Closeness centrality, Security breaches.*

1. Introduction

Network security is an essential element of the contemporary digital environment, where the security and privacy of data, systems, and communication are being subject to ongoing challenges. Due to the fast growth of the internet, and rising dependency on a digital infrastructure, there has been a reversal of cyberattacks of organizations, individuals and governments [1]. These attacks have also taken a new more advanced form whereby they capitalize on the undiscovered vulnerabilities of the network architectures and system protocols [2]. Conventional network security practices although effective to a certain degree will not be effective in curbing the multiplex and dynamic threats experienced in the contemporary interconnected world [3]. This necessitates the introduction of new and more effective approaches in the detection, analysis, and defense against possible threats [4]. As a mathematical concept, graph theory presents an effective method of analyzing and controlling network structure to offer a novel perspective on network security [5].

In this regard, it is important to determine which nodes are critical in a network and evaluate the vulnerabilities order to enhance security in a network [6]. The resilience of a network can be frequently dependent on a number of important characteristics, failure of which would result in extensive failure [7]. The centrality measures, which are graph theoretic measures, enable the identification of such critical nodes - nodes whose failure or compromise may impact network performance and security in disproportionate measure [8]. With the knowledge of the significance of every node in a network and the connection between them, it becomes possible to allocate resources and prioritize defense mechanism better [9]. Besides, network weaknesses that are usually concealed by complicated

topologies can be identified and evaluated through graph-based solutions to construct more effective predictions of attack patterns and the development of more effective recovery plans [10].

The functionality of this study is the simulation and analysis of network topologies using MATLAB. The ability to build network graphs, compute centrality measures, and perform attacks or vulnerability simulation make MATLAB a great solution in dealing with network graphs. The software also enables the analysis of different network setups and orchestration of different security scenarios to determine the effect of the failure or compromise of critical nodes. This paper, through the application of MATLAB, provides an example of the ways in which graph theory could be utilized in relation to practical network security problems, and give practical suggestions on how network resilience and response to changing cyber threats could be better covered.

2. Related Work

Network analysis has been using graph theory, which has provided a strong mathematical system to study the structure and activity of complex systems. Graph theory has become a useful tool to network security [11], especially in the determination of vulnerabilities, detection of anomalous operation and enhancement of network robustness [12]. As has been seen before, graph theory is a useful tool to model and study different types of networks, including computer networks to communication systems [13]. Graph theory can be used to undertake a systemic analysis of network security on the understanding that networks can be represented by graphs, where the nodes can represent the different devices or objects, and the edges can be the links among the different devices in the network on the issue of information flow within them [14]. Numerous studies have been targeted at applying the concept of graph theory to determine the various key nodes, along with their sensitivity, in regards to failed systems of cyber-physical, social and communication networks [15]. The notion of centrality has been extensively applied in order to recognize central nodes that are very important in the global connectivity and functionality of the network [16]. Such metrics as the degree centrality, the betweenness centrality, and the closeness centrality are often used to reveal the nodes that must be considered as the most important to the integrity of the network [17]. One such example is nodes with high betweenness centrality that are at the shortest paths between other nodes and are thus vital in ensuring that there is a flow in the networks [18]. Such node failures or

compromises may have a drastic effect on the activity of networks [19]. On the same note, degree centrality was used to discover nodes with numerous connections and that may act as a bottleneck in case they are attacked. These centrality measures have been utilized in several studies to establish the possible vulnerabilities and rank security resources based on that vulnerability [20]. In this research, the researcher hopes to fill such gaps by implementing graph theory in a more practical, dynamic and scaled manner and combining network data in real-time and giving actionable information to improve network security. Given a combination of both static and dynamic elements of the network topologies and vulnerabilities, this study attempts to provide a more holistic solution to enhancing network resilience.

3. Graph Theory

Graph theory the representation of a graph, on which networks are represented, uses graphs that are represented by vertices (or nodes), and edges (or links). A graph is a mathematical system that can be used to model the pair-wise relationships of objects. The vertices model the objects in the network, which can be computers in communication network, devices in sensor network or users in social network. The edges give the relationship or association between these entities which may be in the form of a physical relationship, communication association or any other

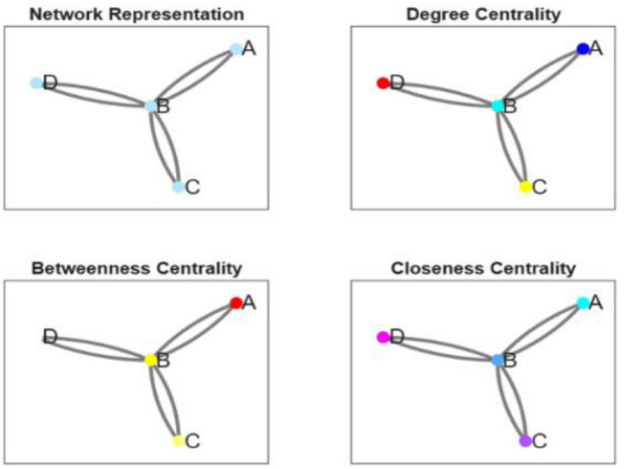

Figure 1

Network Representation and Centrality Measures

association. A network may be directed (the directed edges imply that a particular node of the network sends information to another) or undirected (the directed edges imply that the edges of the network are directed). In directed graphs, the edges are also known as directed edges or arcs which run out of one vertex to the other accounting to the direction of the relationship. In an undirected graph there is however no constancy of direction i.e. mutual relationships between nodes where information or resources can flow in both directions.

The Figure 1 has four subplots, which contain a broader perspective of a network and how it is analyzed using different centrality measures. In the plots outlined earlier the first subplot displays the simplest Network Representation where the nodes (A, B, C, D) are interrelated in terms of edges which depict the basic structure of the network. This is the basis of knowing the relation and network linkage of the various network components. The second subplot is about Degree Centrality where degree centrality determines how different nodes are colored, in this case according to their degree centrality as the number of explicit connections that each node has in the network. Ones that have a large degree centrality are better connected and are essential in ensuring connectivity in the network. Jet colormap is provided to differentiate the nodes based on the centrality scores. The third subplot introduces Betweenness Centrality, which discovers nodes that act as conduits or mouthpiece to other nodes, thus the nodes are very important to restrict the flow of information within the network. The greater betweenness centrality marks the node as an essential node that supports the communication in a network. The nodes have been plotted in hot colormap and brighter colors represent more centrality in betweenness. The fourth subplot demonstrates Closeness Centrality, which is used to determine node closeness to every other node in the network, the efficiency of communication in the network. Vulnerability analysis can be conducted through the analysis of the resilience of the nodes and edges in the case of various attacks, like removal of the nodes or failure of the edges. In such cases, the overall connectivity of the network can be evaluated by applying graph theory techniques to determine the throughput of a network in case of the deletion of critical nodes or edges. Such failures may be measured with the help of graph metrics which can give information about the susceptibility of the network to certain attacks.

4. Methodology

4.1 *Data Collection and Network Topology*

The type of network used in this research is that of a simplified communication network structure that comprises of the nodes linked by the edges. Within the framework of the current study, the network may be a representation of a communication system, where the nodes are represented by computers or devices, or a social network, where they are represented by people and the relationship between them by an edge. In the analysis, we treat the network as an undirected graph, in which each edge includes a connection between two nodes. The graph is constructed in MATLAB using an adjacency matrix, which is a square matrix where each element A_{ij} represents the presence or absence of a connection between nodes i and j. In this study, a simple example of a network is represented by the adjacency matrix.

$$A = \begin{matrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix}$$

The points of the network are represented by every row and column. When a value is 1, then there is a connection (edge) between two nodes whereas when a value is 0, there is no connection. The network structure can be easily visualized and analyzed with the help of this matrix which is used in further calculations.

4.2 *Critical Node Identification*

Centrality measures are used in order to determine crucial nodes and edges in the network. Measures of centrality evaluate the significance of each node based on how central the node is in the network. The three centrality measures, which are commonly used, are: degree centrality, betweenness centrality and the closeness centrality.

Degree Centrality: Centrality of a node is calculated as the degree of the node that is the number of edges of the node. Nodes that have high degree centrality are better connected and, therefore, have more power in the network.

$$\text{Degree Centrality of node i} = \deg(\text{i}) = \sum_j A_{ij}$$

Where A_{ij} is the element of the adjacency matrix indicating the connection between nodes i and j.

Betweenness Centrality: Betweenness centrality of a node is a measurement of how effective the node is in the shortest path between other nodes. High betweenness centrality nodes are considered as bridges between various sections of the network and they are vital in ensuring the flow of the network.

$$\text{Betweenness Centrality of node i} = \sum_{s \neq t \neq i} \frac{\sigma_{st}(i)}{\sigma_{st}}$$

Where $\sigma_{st}(i)$ is the number of shortest paths between nodes s and t passing through iii, and σ_{st} is the total number of shortest paths between s and t.

Closeness Centrality: Closeness centrality determines one node proximity with respect to all the nodes in the network in terms of shortest paths.

$$\text{Closeness Centrality of node i} = \frac{1}{\sum_j d(i.j)}$$

Where $d(i, j)$ is the shortest path distance between nodes i and j

The Figure 2 provides a step-by-step approach to the process of network security analysis, which consists of four important phases. Starting with Data Collection and Network Topology where an adjacency matrix or list is used to represent the network as a graph, all the data on the structure of the network is collected.

Vulnerability Analysis: Vulnerability analysis is about analyzing the effect of the compromise of critical nodes and edges. The vulnerabilities are calculated in this study according to the centrality measurements that were made above. The approach entails deletion or breaking of the nodes that are considered significant (via high centrality rates) and the resultant effect on the network is also looked at with regards to network connectivity and network performance. Graph theory can be used in the modeling of the vulnerability of networks, in that the effect of the deletion of critical nodes or edges can be analyzed as a whole in the structure. When a central node is lost, then the network can be fragmented, and efficiency and connectivity can be lowered. The removal of high-centrality nodes one by one, followed by recalculation of the connectivity of the network based on the adjacency matrix, can be simulated in MATLAB.

4.3 *Simulation Process in MATLAB*

In MATLAB, the centrality measures are calculated and the graph is built with the help of the adjacency matrix, which initiates the process of network simulation. Simulation of network disruptions or attacks is done next by the removal of nodes or edges of the graph.

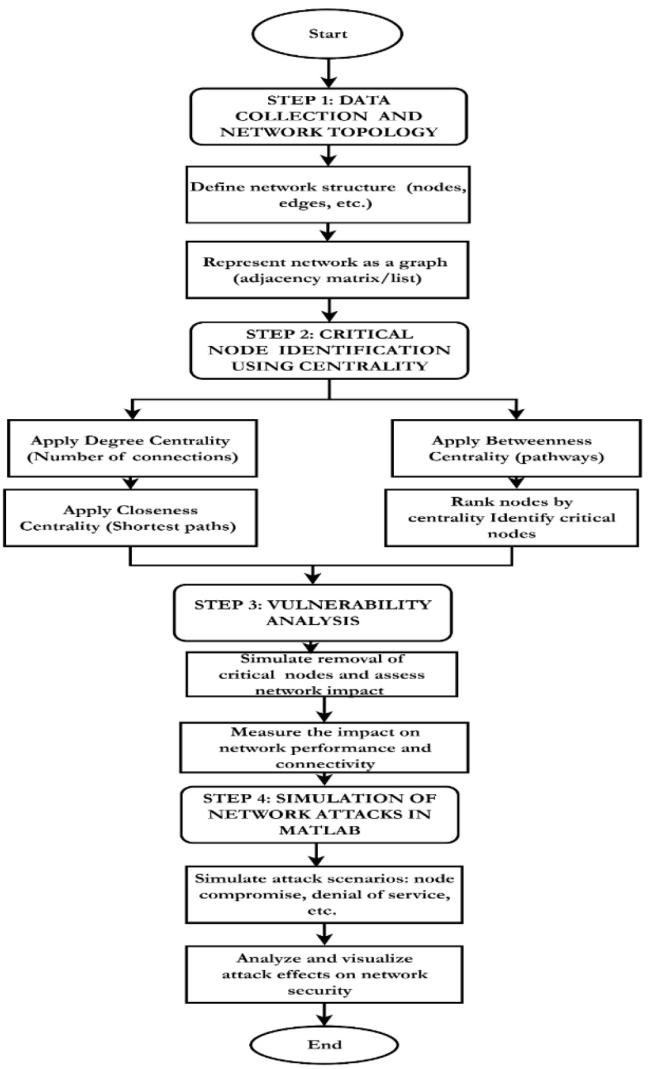

Figure 2

Methodology Flowchart for Network Security Analysis

To illustrate, failure of a node can be represented by assigning a zero to the corresponding row and column in the adjacency matrix and it is effectively removing the node in the network. Graph based analysis in MATLAB is applied to see the effects of deletion of critical nodes on the overall contacts of the network. This is measurable by counting the number of connected pieces having made the disruption. The simulations give information on the possible vulnerabilities of the network and allow prioritizing the nodes and edges that need more security in the network.

5. Results and Discussion

The outputs of the MATLAB simulations indicate that the centrality metrics can be used to determine critical nodes and determine the vulnerability within the system. The key of network topology is displayed in Figure 3 that depicts the network structure in terms of nodes and edges that constitute the structure of the network. Nodes that had high degree centrality (including node B in the example network) were determined by the calculation of centrality measures and these nodes were determined to

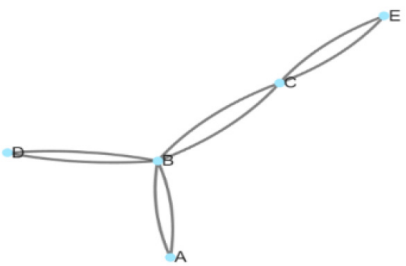

Figure 3
Network Topology

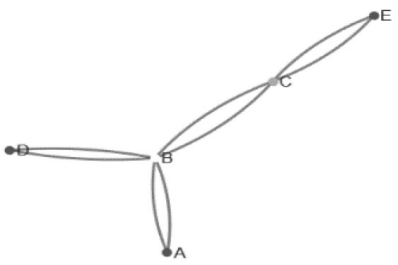

Figure 4
Degree Centrality

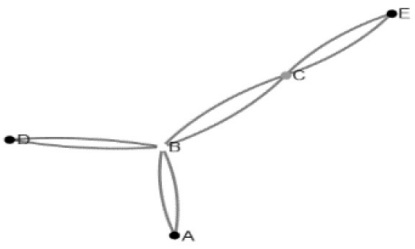

Figure 5
Betweenness Centrality

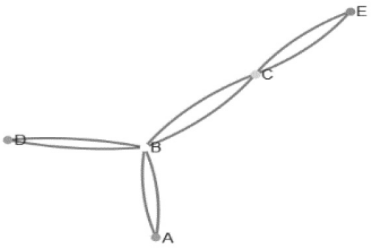

Figure 6
Closeness Centrality

have most direct connections with other nodes and therefore played an important role in keeping the network connected.

The visualization of degree centrality is presented in Figure 4, and the nodes are coloured based on the degree values. The nodes that have the greatest degree centrality are depicted in darker shades, which means that they are the most related and they are the ones much needed by the entire network. Figure 5 and Figure 6 illustrate betweenness centrality and closeness centrality of nodes respectively, having drawn an emphasis on those nodes which can be termed as bridges or closest to the other nodes. These values highlight the role of the nodes that have high centrality in terms of betweenness and closeness, which is crucial to ensure an efficient communication inside the network. Figure 7 is a simulation of the failure (of one node (node B) of the network, which demonstrates how the network is partitioned and broken when a critical node is taken away.

Figure 7

Impact of Node Failure on Network Connectivity

Figure 8

Network Connectivity after Attack Simulation

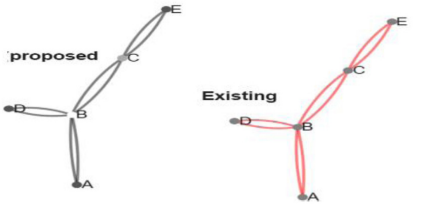

Figure 9

Comparison of Centrality Measures

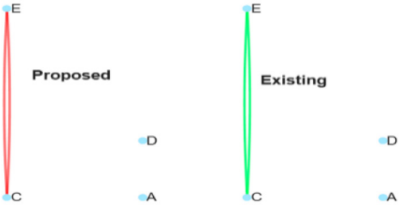

Figure 10

Comparison of Node Failure Impact

Figure 8 is a simulation network with more serious attack scenario by removing several nodes (B and C) of the network, which further affects the connectivity and performance of the network. Such visualizations make it clear how vulnerable the high-centrality nodes are as well as the effect of

the failure on the network. The Figure 9 provides a comparison between the calculation and the visualization of centrality measures (degree, betweenness, and closeness) in our work with the existing approaches. In our implementation, we compute centrality measures based on the centrality of centrality own centrality analysis centrality (input data) as centrality measures along with dynamically displaying centrality measures using color-codings to display nodes in a map type structure which offers a good interactive user-friendly way to understand the significance of each node. The Figure 10 is a comparison of the effects of a node failure in our work and those of the current techniques. Nodes failure simulations are performed in our work by deleting important nodes (e.g. node B) and monitoring the way in which network connectivity and performance is compromised. Current means tend to embrace the dotted analysis of networks explain what can happen as a result because of the failure of the node, which could not be useful to show the chain reactions of the network performance.

The centrality measures were effective in identification of the most vulnerable parts of the network. Degree centrality formed those nodes that are more interconnected and are therefore more susceptible to attacks. The middle nodes like node B which have a high betweenness centrality are critical to the flow of the network and they are important to inhibiting fragmentation. Closeness centrality also gave some information on the nodes that were best able to communicate most to the rest of the network, which made them significant in the reduction of delays and efficient flow of data. The results of the simulation indicate the importance of these centrality measures to network security. Targeted security can be achieved by identification of critical nodes through placing of additional monitoring or protection on high-centrality nodes. The effect of failed critical nodes is a clear evidence of the significance of critical nodes in the network connectivity and security. In relation to the current research, comparing these findings, it can be seen that the measures of centrality have been extensively employed when it comes to the analysis of network vulnerability. Nonetheless, the introduction of the concept of dynamic simulations (the failure of nodes, the attack scenario) introduces a new dimension of understanding network security. Although the previously conducted studies tend to be based on its statics, the present one offers more realistic and dynamic approach to comprehend the network vulnerabilities and enhance standards of its security.

6. Conclusion

In conclusion, the present work has shown that centrality measures can be applied successfully to the network to improve its security on the basis of the graph theory. Using centrality measures like degree, betweenness and closeness centrality, key nodes on the network were determined and the key nodes identified are those that will be at risk of compromise. Simulations in MATLAB revealed that failure of nodes with high centrality which include allies with the highest degree or betweenness centrality played an important role in destabilizing network connectivity. The simulations also demonstrated how these vulnerabilities would result into cascading failures that would impact on the overall network performance. The findings underscore the significance of the high-centrality nodes in terms of security controls in order to make the network resilient. The conclusions made are that dynamic simulations provide a more holistic approach as opposed to conventional fixed systems and this gives in-depth information on actual network vulnerabilities. It can be developed further in future work adding dynamic and adaptive network structures, and also more intricate attack models. Further, the usefulness of graph theory in network security may be increased with further possibilities of its integration with real time information to detect vulnerabilities and recovery mechanisms.

References

[1] G. N. Kannaiyan and R. Veerubommu, "Graph theory matrix approach in cryptography and network security," in *Proc. 2022 Algorithms, Computing and Mathematics Conf. (ACM)*, Chennai, India, pp. 108–110 (2022), doi: 10.1109/ACM57404.2022.00025.

[2] H. A. Dawood, "Graph theory and cyber security," in *2014 3rd Int. Conf. Advanced Computer Science Applications and Technologies*, Amman, Jordan, pp. 90–96 (2014).

[3] I. Boufelgha, M. Ahmia, and M. Guettiche, "Secure 2-domination in graphs," *J. Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 7, pp. 2723–2736 (2025).

[4] N. Khokhlov, S. Kanavin, and A. Rybokitov, "Modeling information security infringements in mobile self-organizing network of communication using fuzzy logic and theory of graphs," in *2019 1st Int. Conf. Control Systems, Mathematical Modelling, Automation and Energy Efficiency (SUMMA)*, Lipetsk, Russia, pp. 60–63 (2019).

[5] Y. Huang and D. Li, "Design of malicious software classification and recognition algorithms based on graph theory in computer networks," in *2024 Int. Conf. Interactive Intelligent Systems and Techniques (IIST)*, Bhubaneswar, India, pp. 593–597 (2024).

[6] A. Torres and G. Anders, "Spectral graph theory and network dependability," in *2009 Fourth Int. Conf. Dependability of Computer Systems*, Brunow, Poland, pp. 356–363 (2009).

[7] F. Zhang and B. Bu, "A cyber security risk assessment methodology for CBTC systems based on complex network theory and attack graph," in *2021 7th Annual Int. Conf. Network and Information Systems for Computers (ICNISC)*, Guiyang, China, pp. 15–20 (2021).

[8] A. S. Odyuo, P. Mercy, and M. K. Patel, "Fibonacci range labeling on direct product and union of graphs," *J. Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 7, pp. 2671–2678 (2025).

[9] W. Jiang, B.-X. Fang, H.-L. Zhang, Z.-H. Tian, and X.-F. Song, "Optimal network security strengthening using attack-defense game model," in *2009 Sixth Int. Conf. Information Technology: New Generations*, Las Vegas, NV, USA, pp. 475–480 (2009).

[10] M. Aouina, H. Karami, and D. J. LaFountain, "Distance-balancing of cube-connected cycles graphs," *J. Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 7, pp. 2849–2861 (2025).

[11] H. Gao, S. Wang, H. Zhang, B. Liu, D. Zhao, and Z. Liu, "Network security situation assessment method based on absorbing Markov chain," in *2022 Int. Conf. Networking and Network Applications (NaNA)*, Urumqi, China, pp. 556–561 (2022).

[12] L. Lima, M. Médard, and J. Barros, "Random linear network coding: A free cipher?" in *2007 IEEE Int. Symp. Information Theory*, Nice, France, pp. 546–550 (2007).

[13] V. Dankan Gowda, N. Suganthi, V. N. Prasad, M. R. Tarambale, P. S. V. V. S. R. Kumar, and A. Muthusamy, "Implementing secure cryptographic protocols in 5G and 6G networks," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 28, no. 5-A, pp. 1505–1515 (2025), doi: 10.47974/JDMSC-2149.

[14] F. Xu, "Design of network attack traceability algorithm based on graph neural network and complex network theory," in *2024 3rd Int. Conf. Artificial Intelligence and Autonomous Robot Systems (AIARS)*, Bristol, United Kingdom, pp. 705–710 (2024).

[15] H. Ge, L. Gu, Y. Yang, and K. Liu, "An attack graph based network security evaluation model for hierarchical network," in *2010 IEEE Int. Conf. Information Theory and Information Security*, Beijing, China, pp. 208–211 (2010).

[16] M. Keramati and A. Akbari, "An attack graph based metric for security evaluation of computer networks," in *6th Int. Symp. Telecommunications (IST)*, Tehran, Iran, pp. 1094–1098 (2012).

[17] D. Man, B. Zhang, W. Yang, W. Jin, and Y. Yang, "A method for global attack graph generation," in *2008 IEEE Int. Conf. Networking, Sensing and Control*, Sanya, China, pp. 236–241 (2008).

[18] V. Dankan Gowda, V. Praveena, M. Nagabhushanam, P. SVVSR Kumar, C. R. Q. Lezama, and D. Pathak, "Homomorphic encryption performance in secure data processing for machine learning," *J. Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1517–1526 (2025).

[19] Q. Xu, S. Yang, L. Xu, and D. Zhao, "Android malware detection method based on graph convolutional networks," in *2024 Int. Conf. Artificial Intelligence and Power Systems (AIPS)*, Chengdu, China, pp. 95–98 (2024).

[20] L. Hailin, W. Yadi, and H. Jihong, "A novel method for modeling complex network of software system security," in *2012 IEEE Sixth Int. Conf. Software Security and Reliability Companion*, Gaithersburg, MD, USA, pp. 24–26 (2012).

Received November, 2025