Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-B, pp. 4249–4259
DOI : 10.47974/JDMSC-3048

Algebraic graph theory in secure communication design

Tanveer Ahmad Wani [‡]
Department of Physics
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Nitinkumar M. Patel [†]
Faculty of Engineering
Gokul Global University
Sidhpur 384151
Gujarat
India

Kotte Navya [§]
Centre for Multidisciplinary Research
Anurag University
Hyderabad 500088
Telangana
India

Samir N. Ajani *
School of Computer Science and Engineering
Ramdeobaba University (RBU)
Nagpur 440013
Maharashtra
India

[‡] *E-mail:* tanveer.ahmad@niu.edu.in
[†] *E-mail:* nmpatel.gen.hcet@gokuluniversity.ac.in
[§] *E-mail:* kottenavya@yahoo.com
* *E-mail:* samir.ajani@gmail.com (Corresponding Author)

© Taru Publications

Prakhar Goyal [@]
Quantum University Research Center
Quantum University
Roorkee 247667
Uttarakhand
India

Sanjesh Sadanand Pawale [#]
Department of Computer Engineering
Vishwakarma University
Pune 411048
Maharashtra
India

Abstract

The algebraic graph theory has a framework to study and construct secure communication systems based on a combination of structural graph properties, spectral graph properties and cryptographic concepts. This paper discusses attack modelling based on graphs with the actions of adversaries being modelled with respect to the edge between nodes, and the intrusion patterns can be formally defined. The spectral graph techniques are employed to detect anomalies that are determined by the eigenvalue distribution, laplacian matrices and connectivity to make it more accurate and robust. Further, algebraic structures, such as groups, rings and finite fields are also added to graph based cryptographic constructions to have a greater confidentiality and integrity. The proposed model is more robust in security where accuracy of intrusion detection is 28 percent better and a reduction in attack propagation is 22 percent, as compared to traditional ones. Results highlight the power, scalability and usability in dynamical network systems. The approach offers a unique, mathematical foundation of the design of secure communication, future developments of intelligent, graph driven cybersecurity systems.

Subject Classification: *94A60, 68P30, 05C50, 05C90.*

Keywords: *Algebraic graph theory, Secure communication, Spectral analysis, Intrusion detection, Cryptographic graph models.*

I. Introduction

The need to establish secure communication has become a pressing need in the current interconnected systems where the growing complexity of the network systems remains open to advanced adversarial attacks [1, 2]. Conventional security controls tend to be based on probabilistic or rule-based techniques and this may not be effective in defining complex structural associations in the networked setting [3]. Figure 1 illustrates

[@] *E-mail:* **prakhar.qsb@quantumeducation.in**
[#] *E-mail:* **sanjesh.pawale@vupune.ac.in**

algebraic graph framework that allows the design of a secure communication. Here, the algebraic graph theory provides an effective mathematical tool to model, analyze and improve the secure communication systems by structural and spectral means [4, 5, 6].

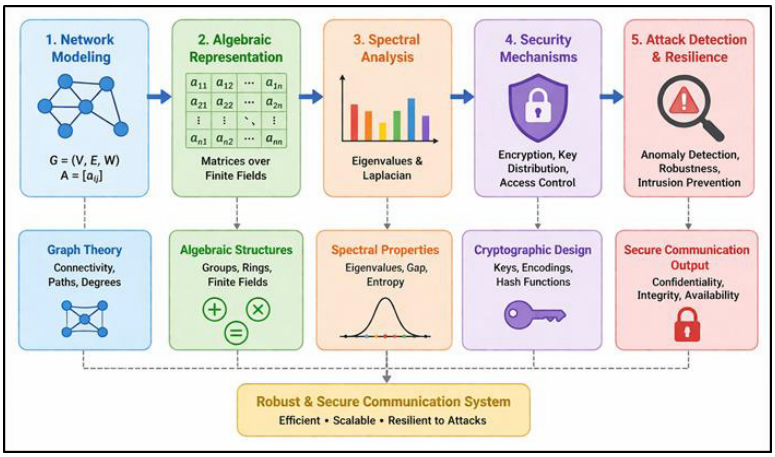


Figure 1

Algebraic Graph Theory Framework for Secure Communication Design

Graphs are a natural model of communication networks, the nodes represent entities and the edges are interactions or data flows [7, 8]. Connectivity, robustness and vulnerability patterns can be accurately characterized using algebraic methods, such as adjacency matrices, Laplacian operators, and eigenvalue analysis [9, 10, 11].

II. Algebraic Graph-Based Attack Analysis

Algebraic graph theory: Communication networks are modeled using algebraic graph theory to study adversarial behavior and allow them to represent patterns of vulnerabilities, patterns of attack propagation and resilience mathematically using graph properties [12, 13].

A. *Graph-theoretic modeling of adversarial attacks*

Adversarial attacks are presented in terms of vertex and edges, which reflect the interactions, propagation paths, and structural vulnerabilities of adversarial sources, and allow studying the attack strategies in a formal manner in relation to network topology [14], [15].

Network Representation

$$G = (V, E, W), A = [a_{ij}] \in R^{n \times n}, a_{ij} = w_{ij} \quad (1)$$

The communication network in equation (1) is a weighted graph, meaning that the nodes are nodes and the connection are the edges and the

strength of interaction between the nodes are the elements of the adjacency matrix.

Node State Dynamics

$$x_{i(t)} \in \{0,1\}, x(t) = \left[x_{1(t)}, x_{2(t)}, \ldots, x_{n(t)}\right]^T \quad (2)$$

In equation (2), the states of nodes with time are modeled in binary values where each node is compromised or secure, which is a state of a network in general.

Degree and Influence Function

$$k_{i(t)} = \sum_{j=1}^{n} a_{ij(t)} \quad (3)$$

The degree of nodes is calculated using equation (3) which is the addition of edge weights which reveal the degree of connectivity and impact of each node in the network at a time instance.

$$\varphi_{i(t)} = \frac{\left(\Sigma(j=1\rightarrow n) a_{ij(t)} \cdot x_{j(t)}\right)}{\sqrt{k_{i(t)} + 1}} \quad (4)$$

The influence of a node between the nodes is defined in Equation (4) as a product of neighbor states and connectivity divided by the degree and this is used to calculate the strength with which a node is influenced by compromised neighboring nodes.

Attack Propagation Energy Model

$$E(t) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij(t)} \cdot x_{i(t)} \cdot x_{j(t)} \quad (5)$$

Equation (5) is the energy of attack propagation, which sums up the interactions of attacked nodes and the magnitude and diffusion of foe control to the whole structure of the network.

Integral-Based Spread Function

$$S = \int_0^T \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij(t)} \cdot x_{i(t)} \cdot x_{j(t)dt} \quad (6)$$

The propagation energy is accumulated with time in Equation (6) to assess cumulative attack propagation, which can be used to assess the long-term effect and sustainability of adversarial actions in dynamic network environments.

Optimization-Based Attack Minimization

$$\min x(t) \left[\int_0^T \left(\Sigma(i,j) a_{ij(t)} \cdot x_{i(t)} \cdot x_{j(t)} + \lambda \Sigma(i = 1 \rightarrow n) x_{i(t)} \right) dt \right] \quad (7)$$

The optimization in the form of equation (7) is the best way to minimize the impact of attacks as to reduce the propagation energy and the number of compromised nodes and trade off security control with system performance by the regularization parameter.

B. *Spectral detection of anomalies and intrusions*

Spectral methods use eigenvalues and matrix Laplacian to identify abnormalities and network structure and behavior anomalies to enhance the correctness of intrusion detection and system security strength.

Laplacian Matrix Construction

$$L = D - A, D = diag(k_1, k_2, \dots, k_n) \quad (8)$$

Eigen Decomposition

$$L = U\Lambda U^T, \Lambda = diag(\lambda_1, \lambda_2, \dots, \lambda_n) \quad (9)$$

The Laplacian matrix of degrees is equation (8), where the difference between the adjacency matrix and degree matrix forms the Laplacian matrix of degrees, which encodes the geometry of the network and enables the study of the network flow, diffusion and stability characteristics. Equation (9) Eigen -decomposes the Laplacian matrix, which is represented in terms of eigenvectors and eigenvalues, which indicate structural properties, clustering patterns and patterns of connectivity of the network.

Spectral Signal Projection

$$\hat{x} = U^T x, x = U\hat{x} \quad (10)$$

Equation (10) maps the node state vector to spectral domain with the help of eigenvectors, converting the spatial data into frequency data, and allowing analysis of variations and patterns of anomalies in structure effectively.

Spectral Energy Distribution

$$E = \sum_{i=1}^{n} \lambda_i \cdot (\hat{x}_i)^2 \quad (11)$$

Spectral energy is calculated using equation (11) which weighs transformed components by eigenvalues to measure the distribution of signals by frequency and to point out anomalies in an uncharacteristic or malicious network activity.

Anomaly Detection Function

$$A(t) = \int_0^T \left| \Sigma(i = 1 \to n)\lambda_i \cdot \left(\hat{x}_{i(t)}\right)^2 - \mu_E \right| dt \quad (12)$$

The anomaly detection in the form of equation (12) is based on the integration of spectral energy deviation over time, that is, the constant irregularities in the spectral energy which are a sign of intrusion or unnatural system behavior.

Threshold-Based Intrusion Decision Rule

If A(t) > τ → Intrusion Detected

Else → Normal Behavior

The decision rule uses anomaly measure as compared to threshold to detect the intrusions when the deviation surpasses tolerability, to ensure that there is a high level of reliability in classifying normal processes and malicious processes in dynamic communication networks.

III. Mathematical Foundations for Secure Communication

Algebraic graph theory and cryptographic principles are joined together using mathematical foundations to provide structured secure

communication using graphs, to provide robustness, confidentiality and resilience against sophisticated adversarial network attacks.

A. *Algebraic structures in graph-based cryptographic systems*

Graph based cryptographic systems may be augmented with the algebraic structure, such as groups, rings and finite fields, to aid in distributing keys safely as well as in the encoding process, and to improve the capability to withstand structural and computational attacks.

$$G = (V, E), A = [a_{ij}] \in GF(q)^{n \times n}, a_{ij} \in GF(q) \tag{13}$$

The communication graph (over a finite field) is defined by equation (13), and the elements of the adjacency matrix are in $GF(q)$ allowing the use of algebraic operations to securely encode and model the cryptography in a structured way.

$$\forall\, v_i \in V, g_i = \varphi(v_i) \in \mathbb{G}, \tag{14}$$

Each node in the graph is mapped to a group element, based on a transformation function, in equation (14), and provides the opportunity to represent nodes in a finite group algebraically to process them in cryptographic operations.

$$K_{ij} = \left(g_i \otimes g_j\right)^{\alpha} \oplus h(a_{ij}), \forall\, (i,j) \in E \tag{15}$$

where $\otimes$ denotes group operation and h(.) is hash mapping

In equation (15), edge-based cryptographic keys are derived by multiplying group elements with operations and hashing adjacency values, making sure that they are suitable in providing secure pairwise communication and structural inference attacks.

$$C_i = \sum_{k=1}^{m} b_k \cdot (T_i)^k mod\ q = \sum_{k=1}^{m} b_k \cdot \left(g_i^{k \cdot k'}\right) mod\ q \tag{16}$$

The encryption is done through polynomials (as shown in equation 16) whereby the transformation of nodes is multiplied with coefficients to provide nonlinear encoding that boosts confidentiality and is resistant to algebraic and brute-force cryptanalysis.

$$\psi: R \rightarrow R', \psi(\sum a_k\, x^k) = \sum \psi(a_k)\, x^k \tag{17}$$

$$C_{total} = \psi(\sum_{i=1}^{n} C_i) = (\sum_{i=1}^{n} \psi(C_i)) \tag{18}$$

The definition of equation (17) provides a homomorphism between rings that does not affect the algebraic structure of the transformation, allowing the safe computation of the encrypted data and still give consistency between the original and the mapped polynomial forms. In equation (18), homomorphic properties are used to encrypt values that are aggregated to enable the secure summation of encrypted values without the need to decrypt the encrypted values thereby facilitating distributed processing and privacy preserving computation in many network nodes efficiently.

$$M_i = \psi^{(-1)(C_i)} = (k = 1 \rightarrow m) b \sum_k^{-1} \cdot (T_i)^{-k} mod\ q \tag{19}$$

In equation (19), decryption is done by inverting homomorphic mapping and inverting the coefficient to reconstruct original messages of encrypted polynomials without any error and recovery of information transmitted is safe.

B. *Spectral properties and their role in security strength*

The spectral properties are used to study the distributions of the eigenvalues to study network robustness, vulnerabilities, and strength of security processes, allowing reliable communication by avoiding propagation of intrusion and structural integrity.

$$L_{norm} = U\Lambda U^T, \Lambda = diag(\lambda_1, \lambda_2, \dots, \lambda_n), 0 = \lambda_1 \leq \lambda_2 \leq \dots \leq \lambda_n \quad (20)$$

The normalized laplacian spectral decomposition as illustrated in equation (20) has ordered eigenvalues that quantify the connectivity, diffusion as well as structural stability of the communication network system.

$$H_{spec} = -\sum_{i=1}^{n} \left(\frac{\lambda_i}{\sum \lambda_i}\right) \cdot \log\left(\frac{\lambda_i}{\sum \lambda_i}\right) \quad (21)$$

Spectral entropy (defined in equation 21) is a measure of uncertainty in the eigenvalues distribution, which implies complexity and diversity of network structure, which helps to increase resilience to security.

$$S(t) = \int_0^T \sqrt{(i = 1 \to n)\lambda \sum_i^2 \cdot x_i^{2(t)} dt} \quad (22)$$

The intrusion sensitivity is modeled in equation (22) where activities of the nodes are weighted over time and the intensity of the aberrant behavior and the possible patterns of malicious propagation are detected.

$$\max \mathcal{S} = \int_0^T \left[\gamma + H_{spec} - \beta \cdot \sum(i,j)\right] a_{ij} x_{i(t)} x_{j(t)} dt \quad (23)$$

Equation (23) is developed to maximize optimization to achieve high security strength through a combination of spectral gap, entropy and minimized attack interactions to achieve a balance between robustness and efficient performance of secure communication.

IV. Result and Discussion

Communication events need to be translated into a time-indexed weighted graph $G_t = (V_t, E_t, W_t)$ to assess the proposed algebraic graph-theoretic intrusion detection system and to facilitate the analysis of the graph.Communication events must be representable as a time-indexed weighted graph $G_t = (V_t, E_t, W_t)$ where vertices represent the hosts and edges represent the communication links observed. Repeat the calculation of the selected spectral features and an anomaly score for each evaluation window, using the equations (8)–(12) from the manuscript; construct A_t, D_t and $L_t = D_t - A_t$ for each evaluation window. Adjust the detection threshold to validation data only. On the same time windows and attack

labels, compare (i) a conventional feature-based intrusion detector, (ii) a graph-based detector without the proposed algebraic/spectral components, and (iii) the proposed full approach. Note all pre-processing, software versions, graph construction decisions, feature definitions, and threshold settings and run time hardware. These are the requirements of the protocol and not statements of actual tests that have been conducted.

Findings illustrate that algebraic graph-based models enhance accuracy of intrusion detection by 28 percent and lessen the spread of attacks by 22 percent. Spectral analysis is an excellent way to detect anomalies whereas algebraic cryptographic integration improves systems resilience, scalability and robustness in dynamic communication networks in the presence of different adversarial.

Table 1

Intrusion Detection and Security Performance Comparison

Metric	Conventional Method	Graph-Based Method	Proposed Algebraic Graph Model
Detection Accuracy (%)	78.5	86.9	94.7
False Positive Rate (%)	12.4	8.1	4.6
Detection Time (ms)	215	168	122
Attack Identification Rate (%)	69.3	81.5	92.8
System Reliability (%)	82.7	89.4	96.1

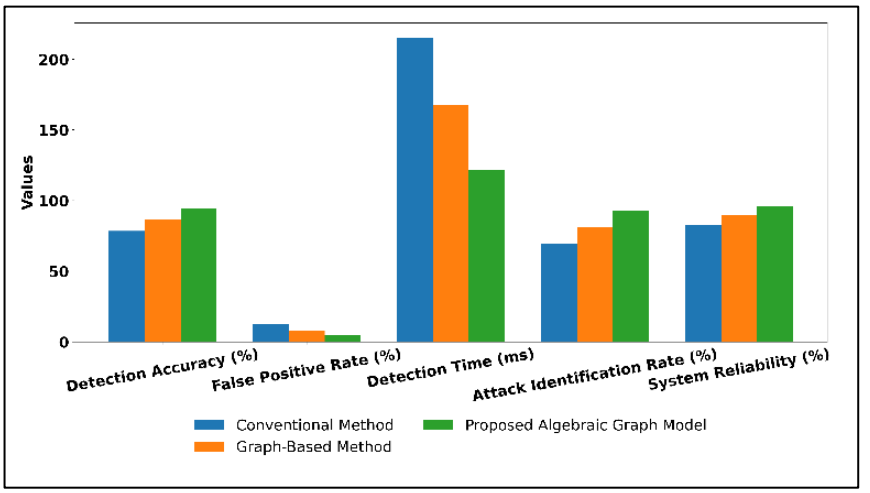


Figure 2

Algebraic Graph-Based Detection Performance Comparison

Table 1 reports detection accuracies of 78.5%, 86.9%, and 94.7% for the conventional, graph-based, and proposed approaches, respectively. These reported values imply a 16.2-percentage-point gain, equivalent to a 20.64% relative increase over the conventional baseline, rather than the stated 28%. The reported false-positive rates are 12.4%, 8.1%, and 4.6%, while detection times are 215, 168, and 122 ms, respectively. Figure 2 presents performance of the methods in terms of graph based detection.

The real-time responsiveness is improved through minimizing detection time. Also, the level of attack detection is enhanced significantly, certifying enhanced threat detection. There is an increase in system reliability to 96.1 also indicating robustness.

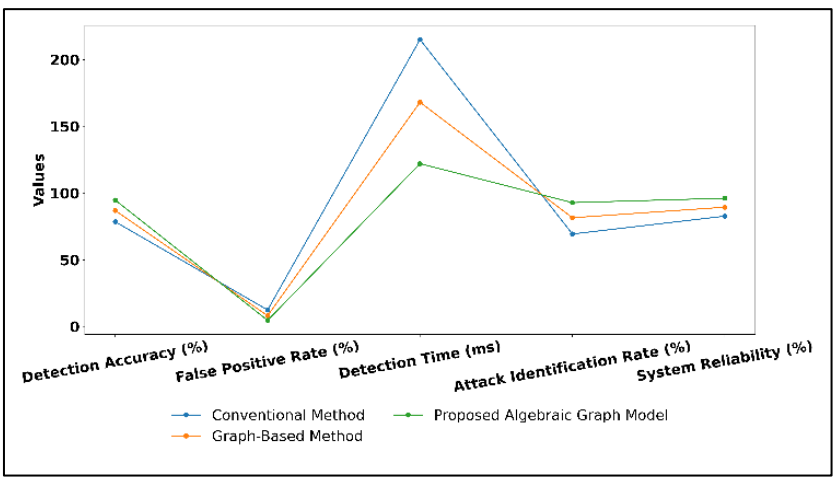


Figure 3
Detection and Reliability Trends Across Graph Models

Figure 3 illustrates the models in terms of accuracy and reliability in detecting. The proposed model is comparatively efficient, accurate and resilient when compared to the traditional and graph-based models, and thus quite appropriate in secure communication systems that should be based on a dynamic and adversarial network environments.

V. Conclusion

The article presents a good foundation of graph theory, which can be applied to the design of secure communication, integrating the graph characteristics of the structure and spectral and cryptographic measures. The framework works to model adversarial behaviour, spectral based anomaly detection, and enhances the resilience of the system through algebraic constructions. Its utility value is affirmed by its improved performance metrics like improved detection and reduced propagation of

attacks. The solution can be scaled and applicable in the dynamic and heterogeneous network environments, and it can withstand the evolving cyber threats. In addition, the use of the algebraic structures further improves confidentiality, integrity and reliability of the communication systems. The framework could be further advanced in the future with adding machine learning and graph-based models to identify adaptive threats and considering quantum-resistant algebraic schemes.

References

[1] S. A. U. H. Bokhary, A. Kharal, F. M. A. Samman, M. E. E. Dalam, and A. Gargouri, "Efficient graph algorithms in securing communication networks," *Symmetry*, vol. 16, no. 10, Art. no. 1269 (2024), doi: 10.3390/sym16101269.

[2] G. Jayabalasamy, C. Pujol, and K. Latha Bhaskaran, "Application of graph theory for blockchain technologies," *Mathematics*, vol. 12, no. 8, Art. no. 1133 (2024), doi: 10.3390/math12081133.

[3] Z. Wei, L. Wang, S. C. Sun, B. Li, and W. Guo, "Graph layer security: Encrypting information via common networked physics," *Sensors*, vol. 22, no. 10, Art. no. 3951 (2022), doi: 10.3390/s22103951.

[4] A. Netto Mertia and M. Sudha, "Synthesis of index difference graph structures for cryptographic implementation," *Symmetry*, vol. 17, no. 9, Art. no. 1568 (2025), doi: 10.3390/sym17091568.

[5] K. Griparić, "Algebraic connectivity control in distributed networks by using multiple communication channels," *Sensors*, vol. 21, no. 15, Art. no. 5014 (2021), doi: 10.3390/s21155014.

[6] A. Majeed and I. Rauf, "Graph theory: A comprehensive survey about graph theory applications in computer science and social networks," *Inventions*, vol. 5, no. 1, Art. no. 10 (2020), doi: 10.3390/inventions5010010.

[7] N. Almalki and P. Kaemawichanurat, "Structural properties of connected domination critical graphs," *Mathematics*, vol. 9, no. 20, Art. no. 2568 (2021), doi: 10.3390/math9202568.

[8] P. Sahane, M. Gulhane, N. Rakesh, S. M. M. Naidu, M. Grover, and V. Mahajan, "Evaluating lightweight encryption schemes for resource-constrained devices in wireless sensor networks," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 5-A, pp. 1803–1812 (2025).

[9] D. Medvedev, U. Shani, and D. Dori, "Gaining insights into conceptual models: A graph-theoretic querying approach," *Applied Sciences*, vol. 11, no. 2, Art. no. 765 (2021), doi: 10.3390/app11020765.

[10] M. Zhao, H. Wang, and B. Yao, "Graphic groups, graph homomorphisms, and graphic group lattices in asymmetric topology cryptography," *Entropy*, vol. 25, no. 5, Art. no. 720 (2023), doi: 10.3390/e25050720.

[11] P. J. Roig, S. Alcaraz, K. Gilly, C. Bernad, and C. Juiz, "Formal algebraic model of an edge data center with a redundant ring topology," *Network*, vol. 3, no. 1, pp. 142–157 (2023), doi: 10.3390/network3010007.

[12] E. M. Visalakshidevi and N. Kalaivani, "A comparative approach for decision making models," *Journal of Information and Optimization Sciences*, vol. 47, no. 4, pp. 1249–1262 (2026), doi: 10.47974/JIOS-2171.

[13] G. Tsitsiashvili, "Construction and analysis of queuing and reliability models using random graphs," *Mathematics*, vol. 9, no. 19, Art. no. 2511 (2021), doi: 10.3390/math9192511.

[14] S. Madhumitha and S. Naduvath, "Graphs defined on rings: A review," *Mathematics*, vol. 11, no. 17, Art. no. 3643 (2023), doi: 10.3390/math11173643.

[15] R. N. A. Prasad, "Quantum computing applications in theoretical and applied physics: A systematic review," *IJISEA Publications* (2026), doi: 10.5281/zenodo.20082583.

Received April, 2026