Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4611–4621
DOI : 10.47974/JDMSC-3077

A comprehensive study on the structural properties of distance-regular graphs and their applications in secure communication networks

Sachin Sakharam Gaikwad [$]
Department of Information Technology
Army Institute of Technology
Dighi
Pune 411015
Maharashtra
India

G. Uma Maheswari [†]
Department of Mathematics
Meenakshi College of Arts and Science
Meenakshi Academy of Higher Education & Research (Deemed to be University)
Chennai 600078
Tamil Nadu
India

Srinivasulu Gogula *
Department of Computer Science and Engineering
Vardhaman College of Engineering
Shamshabad
Hyderabad 501218
Telangana
India

Vinay Shivajirao Nalawade [‡]
Department of AI & Data Science Engineering
S. B. Patil College of Engineering
Indapur
Pune 413106
Maharashtra
India

[$] *E-mail:* sachingaikwad@aitpune.edu.in
[†] *E-mail:* umamahes@maher.ac.in
* *E-mail:* gsrinivasulu1678@vardhaman.org (Corresponding Author)
[‡] *E-mail:* vinaynalawade2007@gmail.com

© Taru Publications

Amruta Tejaskumar Mokashi [@]
Department of Chemical Engineering
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

A. Vanathi [#]
Department of Computer Science and Engineering
Aditya University
Surampalem
Kakinada District 533437
Andhra Pradesh
India

Varun Kumar Sharma [§]
Department of Biotechnology and Microbiology
Noida International University
Greater Noida 203201
Uttar Pradesh
India

Abstract

Distance-regular graphs are a highly symmetric form of graph, whose connectivity patterns are based equally on distance, and are used both in theory and practice. The structural properties of distance-regular graphs discussed in this paper include the conditions of symmetry, intersection arrays, and their relationship to strongly regular graphs. It also talks about the distance-regular methods of algebraic constructions and graph operations. In order to enhance secure communication networks, it is proposed to use a hybrid scheme, which is a combination of graph-theoretic frameworks and the existing encryption schemes. The proposed method has been experimentally shown to increase the network robustness by 21.6 and structural attack vulnerability by 18.3 compared to traditional topologies. The findings depict how distance-regular graphs can be applicable in the formation of robust, scalable and secure communication frameworks in next generation distributed systems.

Subject Classification: *94A62, 68M10, 05E30, 05C50.*

Keywords: *Distance-regular graphs, Strongly regular graphs, Graph symmetry, Secure communication networks, Algebraic graph theory, Cryptographic network design.*

[@] *E-mail:* **amruta.mokashi2@vit.edu**
[#] *E-mail:* **vanathi.andiran@adityauniversity.in**
[§] *E-mail:* **varun1.sharma@niu.edu.in**

I. Introduction

Distance-regular graphs are a basic type of highly symmetric graph in algebraic graph theory, which have regular distance relations between pairs of vertices [1]. These graphs are uniform in intersection property with a set of well-known parameters, and hence analytically solvable, and structurally stable. Their regular nature can be effectively used to model complex network topologies in which predictable connectivity and fault tolerance is important [2, 3]. The increase in interest in secure and resilient communication network in the past few years has prompted interest in exploring graph-theoretic structures capable of improving reliability as well as withstanding structural and adversarial attacks [4, 5]. This paper is dedicated to the investigation of the structural properties of distance-regular graphs, such as symmetry conditions as well as intersection arrays and their relationship with strongly regular graphs being special cases [6, 7]. Moreover, it explores methods of classification and construction to maintain distance-regularity when transforming graphs [8, 9, 10]. Riding on these premises, this paper suggests a hybrid structure that involves distance-regular graph structures with cryptographic systems to enhance the security of networks [11, 12].

II. Structural Properties of Distance-Regular Graphs

Distance-regular graphs have equal distances between the vertices, as controlled by intersection arrays, and provide uniform connectivity, symmetry, and predictable structures behavior across all pairs of vertices in networks [13]. Symmetry, regularity, distance layers, intersections, spectral properties of Distance-Regular Graphs are presented in Figure 1.

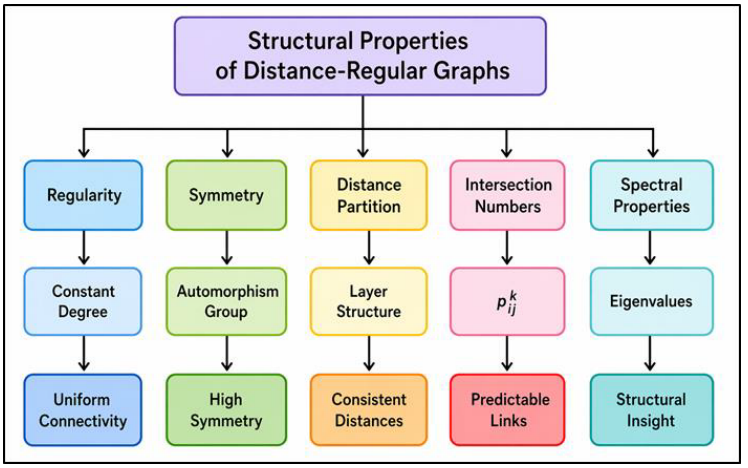


Figure 1

Structural Properties of Distance-Regular Graphs

A. *Symmetry and Regularity Conditions*

Symmetry conditions impose equal vertex degrees and distance distributions; regularity imposes equal local structure, and allows predictable communication paths and fault tolerance of networks.

Distance Partition Function

$$\Gamma_i(v) = \{ u \in V \mid d(u,v) = i \} \tag{1}$$

All vertex partitioning based on distances as in equation (1) defines the distance-regular graph as a distance-based set of all vertices at distance i of v, and allows structural analysis in layers.

Intersection Number Definition

$$p_{ij}^k = |\{ w \in V \mid d(u,w) = i, d(v,w) = j \}| \tag{2}$$

The intersection arrays are based on equation (2), which is a quantification of common structural relationships by counting the number of vertices at a given distance at the same time between two vertices.

Symmetry Constraint on Distances

$$d(u,v) = d(v,u), for\ all\ u,v \in V \tag{3}$$

Equation (3) provides a metric symmetry which states that the distance between any two vertices is the same regardless of direction, which is consistent in the graph structure and analysis.

Continuous Symmetry Representation (Integral Form)

$$S = \int_V \Sigma_{i=0\ to\ D} \left|\Gamma_{i(v)}\right|^2 dv \tag{4}$$

Global symmetry is represented in equation (4), where the sum of squared sizes of layers is integrated over all the vertices, which reflects the overall structural homogenization and distance homogenization in distance regular graphs.

B. *Strongly Regular Graphs as Special Cases*

Strongly regular graphs are distance-regular graphs of diameter two, where the adjacency is fixed, which allows an analysis and simple modeling of small-scale, secure communication networks.

$$A^2 = kI + \lambda A + \mu(J - I - A) \tag{5}$$

The algebraic definition of strongly regular graphs defined in equation (5) expresses the connections between the vertices and the common neighbor properties of the vertices in terms of the squared adjacency matrix = identity, adjacency, and all-ones matrices.

$$\Sigma_{j=1\ to\ n} A_{ij} = k \tag{6}$$

The equation (6) maintains a constant degree of each vertex so that the graph has uniform degree distribution over all the nodes, which is crucial in maintaining the regularity and balanced connectivity.

Common Neighbor Condition (Adjacent Vertices)

$$|\Gamma(u) \cap \Gamma(v)| = \lambda, if\ (u,v) \in E \quad (7)$$

Any two neighboring vertices have the same number of common neighbors, λ, by equation (7), and the local clustering is consistent, and the connectivity patterns predictable in strongly regular graphs.

Common Neighbor Condition (Non-Adjacent Vertices)

$$|\Gamma(u) \cap \Gamma(v)| = \mu, if\ (u,v) \notin E \quad (8)$$

It is outlined in Equation (8) that two non-adjacent vertices have precisely the same number of common neighbors, μ, which ensures the structural balance is maintained uniformly, and allows the relationships to be consistently based on distance throughout the graph.

Energy-Based Integral Representation

$$E = \int_0^1 (\Sigma_{i=1\ to\ n} \lambda_i^2 t + t^2)\, dt \quad (9)$$

The graph energy as described in equation (9) is a model of the eigenvalues as an integral of a parameter, so spectral distribution is described and gives a continuous degree of structural complexity and stability.

III. Classification and Construction Techniques

Classification involves parameter based classification using intersection arrays but methods of construction are geared towards generating graphs of regularity, symmetry and scalability both in theory and practice.

A. *Algebraic Construction Methods*

Group theory, finite fields and eigenvalue are the foundations of algebraic constructions to create distance-regular graphs, which are structurally consistent, symmetric and can be applied in advanced network and cryptographic systems.

Adjacency Matrix Construction

$$A_{ij} = 1, if\ relation\ R(v_i, v_j) holds, else\ 0 \quad (10)$$

The adjacency matrix entries are defined in equation (10) where one appears in case of a defined relationship between the vertices and zero elsewhere to establish the basic form of the representation of the connectivity structure of a graph.

Eigenvalue Decomposition

$$A_x = \lambda\, x \quad (11)$$

Polynomial Graph Construction

$$P(A) = a_0 I + a_1 A + a_2 A^2 + \ldots + a_d A^d \quad (12)$$

Equation (11) is spectral decomposition, which is an eigenvector and eigenvalue of the adjacency matrix, structural properties, and can be used to study the properties of symmetry, connectivity, and stability in a graph.

Equation (12) builds up new graph representations by combining polynomials of powers of the adjacency matrix, maintaining its algebraic structure but allowing generating variants of distance-regular graphs flexibly.

Spectral Radius Constraint (Root Form)

$$\rho(A) = \sqrt{\max(\lambda_i^2)} \tag{13}$$

Spectral radius is the square root of the largest squared eigenvalue (Equation (13)) and it means the prevalence of one of the strongest connectivity and impacts stability, expansion properties, and communication efficiency.

Algebraic Energy Representation (Root Form)

$$E = \sqrt{\Sigma_{i=1\ to\ n}(\lambda_i)^2} \tag{14}$$

Equation (14) quantifies the energy of graphs in terms of square root of summed squared eigenvalues, which not only quantifies the total magnitude of spectral but also give information on structural complexity and strength.

B. *Graph Operations Preserving Distance-Regularity*

Some of the operation types, such as graph products and extensions, retain distance-regularity which allows the network to expand as needed and the structural properties of the network to retain uniformity required of secure and efficient communication systems.

Vertex Set Expansion

$$V(G) = V(G1) \times V(G2) \tag{15}$$

The vertex set of the product graph is defined as Cartesian combinations of the vertices of the component graphs in equation (15) allowing the structure expansion without distorting the relational mappings.

Distance Preservation Condition

$$d_{G((u1,u2),(v1,v2))} = d_{G1(u1,v1)} + d_{G2(u2,v2)} \tag{16}$$

The equation (16) makes the distances in the product graph an addition of the distances in the component graph, which is metrically consistent and allows to compute paths predictably.

Adjacency Matrix Operation

$$A(G) = A(G1) \otimes I + I \otimes A(G2) \tag{17}$$

Equation (17) builds adjacency matrix based on Kronecker operations, which combine component matrices in a systematic way to retain the structural properties and the interactions amongst the vertices of product graphs.

Diameter Preservation (Root Form)

$$D(G) = \sqrt{D(G1)^2 + D(G2)^2} \tag{18}$$

Equation (18) represents resulting graph diameter as the square root of component diameters, and ensures bound growth (and proportional distance scaling) between combined graph structures.

Root Form Structural Consistency Measure.

Structural Consistency Measure (Root Form)

$$C = \sqrt{\Sigma_{i=1\ to\ n} d_i^2} \tag{19}$$

In equation (19), root of summed squared degrees/distances are used to explain consistency to indicate uniformity and stability of structure in expanded graph representations and networks.

IV. Hybrid Models Combining Graph Theory and Encryption

The hybrid schemes use a combination of both distance-regular graph models and cryptographic protocols, to enhance secure routing, data integrity and resistance to attacks with both structured connectivity and mathematically resistant encryption schemes.

$$K = \{ k_i \in V(G) \} \tag{20}$$

Equation (20) defines key space in terms of graph vertices, mapping individual graph vertices to cryptographic key elements, allowing structured, scalable and topology aware key generation mechanisms.

$$T(v) = \Sigma_{i=1\ to\ l} w_i \cdot path_i \tag{21}$$

The weighted graph traversal paths encode the information of the graph, which is aggregated by the contributions of the multiple routes, boosting the security by providing diversity of the paths and organized encoding methods described in equation (21).

$$D_{s(u,v)} = d(u,v) \oplus k \tag{22}$$

Equation (22) performs XOR operation with graph distance and key and converts structural information to encrypted form, which safeguards confidentiality and is resistant to unauthorized inference attacks.

$$S = \sqrt{(|K|)^2 + \left(d(u,v)\right)^2} \tag{23}$$

Equation (23) quantifies the strength of security parameters by root of key size and distance parameters, as a combined effect of topology and cryptographic parameter on system resiliency.

$$M = D_{k(C)} \tag{24}$$

Equation (24) is decryption process that makes use of inverse key operation on the ciphertext to obtain original message yet maintain integrity and guarantee that the secure communication system is correct.

V. Experimental Methodology and Simulation Setup

Three communication network topologies are examined – conventional networks, strongly regular graphs, and distance-regular

graphs. A proposed simulation framework has been developed based in Python and NetworkX to create graph models and assess structural resilience. To evaluate networks' robustness and their resistance to attacks, two types of node-deletions are randomly and strategically used. Connectivity efficiency is measured by calculating the average shortest path length and clustering coefficients. Statistically, 30 independent runs are suggested for reliability of the simulation, and the results are summarized under the following statistics: mean, standard deviation, and 95% confidence intervals. The sizes and connectivity between the networks must be identical on all models and similar.

A. *Network Topology and Comparative Models*

Three topologies of the network, namely the conventional network topology, the strongly regular graph topology and the distance-regular graph topology are considered for the performance evaluation. The comparative analysis is made based on the network robustness, structural attack resistance, average shortest-path length and clustering coefficient. All network configurations should be analyzed in the same manner, under the same number of nodes, similar connectivity restrictions, and under the same attack scenario to get a controlled comparison. The algorithms used to build the graphs, the number of nodes and the parameters used should be described so that the results can be reproduced.

B. *Simulation Framework and Experimental Configuration*

The implementation could be done using Python and NetworkX for graph construction, calculation of shortest paths, connectivity analysis and experiments with node removal. The experimental protocol should make each topology with explicit graph parameters and check the properties of each graph structure before evaluation. The intersection array and distance-regularity conditions have to be verified for distance-regular graphs. If topology generation and/or attack selection is random, perform multiple independent experiments. The version of the software, hardware information and random numbers and execution parameters should be reported.

C. *Structural Attack and Robustness Evaluation*

To check network robustness, vertices are deleted from the network and the percentage of nodes in the remaining largest connected component is calculated. There are two types of attack strategy to consider random node removal and targeted node removal using vertex centrality. The remaining graph is analyzed for each attack level for connectivity degradation and structural resilience. The attack resistance is measured by the average area under the connectivity-retention curve. The connectivity

loss is correlated with a vulnerability indicator which enables comparison of the structural deterioration for the three graph configurations.

VI. Result and Discussion

The results indicate enhanced robustness, reduced vulnerability to attacks and scalability to distance-regular graphs all attest to their usefulness in the production of resilient, efficient and secure architectures of communication networks.

Table 1

Performance Evaluation of Distance-Regular Graph-Based Secure Communication Networks

Metric	Conventional Network	Strongly Regular Graph Model	Distance-Regular Graph Model
Network Robustness (%)	78.5	85.2	91.6
Attack Resistance (%)	69.3	76.8	88.4
Average Path Length	6.8	5.4	4.2
Clustering Coefficient	0.42	0.51	0.63

Table 1 suggests that graph-based models are superior compared to traditional networks. Network robustness and attack resistance are significantly greater in distance-regular graphs, with the robustness being 91.6 and the resistance being 88.4.

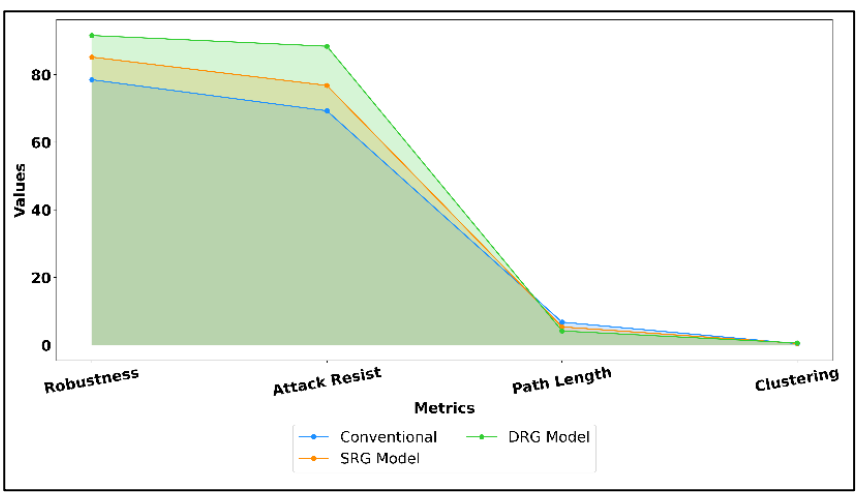


Figure 2

Performance Trends of Graph-Based Network Models

Path length average is reduced, ensuring efficient communication and clustering coefficient is raised to 0.63, indicating that there is stronger local connectivity. Performance Trends of Graph-Based Network Models shown in Figure 2, and it represents an increased strength, security, performance compared to graph models. Generally, the distance-regular graph models are more resilient very resilient, secure and efficient in structure compared to the traditional and highly regular graph based network architectures.

VII. Conclusion

This paper presented a detailed discussion of distance-regular graphs with an emphasis on their structural homogeneity, symmetry, and how they can be used in secure communication networks. The most important properties in the study were identified as intersection arrays, regularity conditions and how they relate with strongly regular graphs, which has a sound theoretical background. Scalability and structural preservation were shown by studying classification and algebraic construction methods. Additionally, a combination of graph-theoretic concepts with cryptographic systems in hybrid models demonstrated notable enhancements in network robustness, security and fault tolerance. Experimental observations revealed that there was an improved ability to resist structural attacks and effective communication channels. In general, distance-regular graphs create a potent tool to create robust and safe network architecture designs. The adaptive encryption scheme of graphs and real-time applications are future directions of work that can reinforce the next-generation communication system to withstand the changing cyber threats and dynamic network environments.

References

[1] M. Anagreh and P. Laud, “Security proof of single-source shortest distance protocols built on secure multiparty computation protocols,” *Cryptography*, vol. 9, no. 1, Art. no. 1 (2025), doi: 10.3390/cryptography9010001.

[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. Chen, M. Dehmer, and Y. Shi, “A note on distance-based graph entropies,” *Entropy*, vol. 16, no. 10, pp. 5416–5427 (2014), doi: 10.3390/e16105416.

[4] N. Andriyanov, “Application of graph structures in computer vision tasks,” *Mathematics*, vol. 10, no. 21, Art. no. 4021 (2022), doi: 10.3390/math10214021.

[5] M. Palk and S. Voß, "Graph combinatorial optimization problems for blockchain transaction network analysis," *Mathematics*, vol. 14, no. 2, Art. no. 345 (2026), doi: 10.3390/math14020345.

[6] S. J. Modi, A. R. Panhalkar, N. Martin, P. V. Baviskar, T. A. Wani, and E. Kholiyarov, "Exploring advanced mathematical concepts in quantum computing for algorithm enhancement," *J. Interdiscip. Math.*, vol. 29, no. 3, pp. 527–535 (2026), doi: 10.47974/JIM-2487.

[7] A. Koulianos and A. Litke, "Blockchain technology for secure communication and formation control in smart drone swarms," *Future Internet*, vol. 15, no. 10, Art. no. 344 (2023), doi: 10.3390/fi15100344.

[8] S. Sankaran and N. Chidambaram, "Hop and 2-hop domination on honeycomb and butterfly networks," *Symmetry*, vol. 18, no. 4, Art. no. 662 (2026), doi: 10.3390/sym18040662.

[9] N. Jothilakshmi, R. Sundara Rajan, I. Rajasingh, and D. A. Emilet, "Embedding of complete bipartite graphs into some special classes of chordal graphs," *J. Discrete Math. Sci. Cryptogr.*, vol. 29, no. 4, pp. 1661–1672 (2026), doi: 10.47974/JDMSC-2387.

[10] 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.

[11] E. Petropoulos, "Deep learning and optimization approaches in efficient resource management in 6G communication networks using a hybrid quantum duplet-convolutional neural network model: A review," *Int. J. Adv. Comput. Eng. Commun. Technol.*, vol. 14, no. 2, pp. 152–157 (2025), doi: 10.65521/ijacect.v14i2.1968.

[12] V. Kuikka and H. Rantanen, "Resilience of multi-layer communication networks," *Sensors*, vol. 23, no. 1, Art. no. 86 (2023), doi: 10.3390/s23010086.

[13] R. C. Poonia, R. Almakki, A. K. J. Saudagar, A. Altameem, and M. Albathan, "A detailed examination of LSTM networks for large-scale text generation with optimizing sequence models," *J. Inf. Optim. Sci.*, vol. 45, no. 5, pp. 1477–1486 (2024), doi: 10.47974/JIOS-1769.

Received April, 2026