A Novel Approach to Secure Distance Matrix Domination in Fundamental Graphs

Dr.M Nazreen Banu[1], Dr. Pankit S. Gandhi[2], C. Ruby Sharmila[3], A.Atkinswestley[4], J. Juli Amala Rani[5], G. Suganthi[6], Dr.B.Sivasankari[7]

[1]Associate Professor, Department of Mathematics, Thassim Beevi Abdul Kader College for Women, Ramanathapuram, Email: nazreenmathematics@gmail.com
[2]Associate Professor, Department of Mathematics, Kishinchand Chellaram College, Mumbai, Email: pankit.gandhi@kccollege.edu.in
[3]Assistant Professor, Department of Mathematics, Tamilnadu College of Engineering, Coimbatore, Email:sharmilaruby1312@gmail.com
[4]Associate Professor, Department of Mathematics, K.Ramakrishnan College Of Engineering, Tiruchirapalli, Email:ats.wesly@gmail.com
[5]Assistant Professor, Department of Mathematics, Panimalar Engineering College, Chennai, Email: jesujuli@gmail.com
[6]Assistant professor, Department of Mathematics, Sona College of Technology, Salem, Email:sugachandru@gmail.com
[7]Professor (Mathematics), Department of Agricultural Economics, Agricultural College and Research Institute, Madurai , Email :sankari83@tnau.ac.in

Received: 13.07.2024 Revised: 15.08.2024 Accepted: 22.09.2024

ABSTRACT
Distance matrix domination in fundamental graphs plays a critical role in various applications, such as network design, communication systems, and social network analysis. Ensuring the security of these distance matrices is essential to protecting the integrity and privacy of the underlying graph structure. This paper presents a novel approach to secure distance matrix domination by integrating advanced cryptographic techniques and privacy-preserving mechanisms.We propose the use of homomorphic encryption to allow computations on encrypted distance matrices, safeguarding data while maintaining functionality. Additionally, secure multi-party computation (MPC) enables collaborative domination in distributed networks without revealing individual node or edge data. To further protect graph structure, we employ graph perturbation techniques and differential privacy, ensuring that sensitive details about the graph are not exposed.Randomized shortest path computations are introduced to obscure direct inferences about the graph's topology, while zero-knowledge proofs (ZKP) allow verification of domination results without revealing the distance matrix. A decentralized framework leveraging blockchain ensures that the domination process remains transparent and secure. Finally, machine learning algorithms are integrated for real-time anomaly detection, enhancing the robustness of the domination process against adversarial attacks.This novel approach enhances the security and privacy of distance matrix domination in fundamental graphs, making it applicable to sensitive and large-scale network environments. The proposed methods ensure both accuracy and confidentiality, offering a significant advancement in secure graph analysis and optimization.

Keywords: Domination, Dominating set, Secure distance matrix domination, Distance domination, complete graph.

1. INTRODUCTION

Dominance is a crucial subfield of graph theory, with roots tracing back to 1862 when Campbell [1] explored the problem of determining how many queens are required to dominate a chessboard. The study of dominating sets in graphs formally emerged in the 1960s and has since been a central topic in graph theory research. The notion of dominance in graphs, denoted by G=(V,E) where V is the vertex set and E the edge set, investigates how certain vertices, called dominant vertices, can "control" others within a graph. The concept was first introduced as a graph-theoretic term by Berge and Ore [2], with Ore also coining the terms "dominant set" and "domination number."

A set $D \subseteq V$ is called dominant if every vertex not in D is adjacent to at least one vertex in D. The minimal size of such a set is known as the domination number $\gamma(G)$. The study of dominating sets has broad

applications, ranging from network control to social network analysis. A significant challenge in this area arises when one seeks to ensure secure domination, particularly in distributed or sensitive environments, where exposing the structure of the graph or the domination process could lead to vulnerabilities.

Recent advancements have expanded the concept of domination by introducing secure domination, which guarantees that domination is preserved even if vertices or edges are compromised. Cockayne et al. [13] introduced the idea of secure domination, which has been extensively studied in various contexts [14–17]. Secure domination ensures that if a vertex in the dominating set is removed, its role is taken over by another vertex, thereby maintaining domination integrity.

An essential subfield of graph theory is dominance. Investigating dominant initiates within graphs dates back to 1862, when Campbell [1] investigated the issue of figuring out how many queens are required to control a chessboard. The field of research of dominating sets in graphs came into being about 1960. The centre of graph theory study has been the theory of dominance.Within known as $G* = (V*, E*)$ a graph, Assume that the point set is V* and the border set is $E*$.The investigation of being dominant establishes takes up a large amount of roomthrough the field of graph theory. The dominance was first introduced as a graph theoretic concept by C. Berge and O. Ore [2].

The phrases "dominant set" and "domination number" were also created by O. Ore [2]. Place $D*$ is an extremely powerful set, or within close proximity of dominance$D_{SDM}\, N_d[D*] = D_{SDM}\, V*$ [3], As long as every vertex is present in $D_{SDM}\, V* - D_{SDM}\, D*$has become located adjacent to any vertex within$D_{SDM}\, D*$.If and only if no edge connects any two of the vertices of a graph with the same number of vertices, V*(G*), it is referred to as the complement graph of a simple graph G* [4].

If every point in $D_{SDM}\, G*$ the fact that does not exist in $D_{SDM}\, D*$ is close to at least one of the vertices in $D_{SDM}\, D*$, and then $D_{SDM}\, G*$ represents the being dominant set.The lowest possible cardinality of a set that dominates in $D_{SDM}\, G*$ is equal to the dominance the number $D_{SDM}\, (\gamma*(G*))$.In the event there are no two vertices that are close together in set $D_{SDM}\, S* \subset D_{SDM}\, V*$, then set S is independent.A peak performance independent determined by $D_{SDM}\, G*$ has a pair of minimum and maximum cardinalities whose respective values equivalent the degree of independence number $D_{SDM}\, (\beta_0(G*))$as well as a dominant number ascertained independently$D_{SDM}\, (i(G*))$.

This paper introduces a novel approach to secure distance matrix domination, which builds on traditional domination theory but incorporates cryptographic techniques and distance parameters to enhance security. We explore the application of secure multi-party computation (MPC) and homomorphic encryption to protect the underlying graph structure. Additionally, we propose decentralized control and privacy-preserving methods, such as differential privacy and graph perturbation, to mitigate risks.

The concept of distance matrix domination further refines traditional dominance by incorporating distance-based criteria, ensuring that dominating vertices are within a certain distance of each vertex in the graph. This is particularly relevant in large-scale networks, where direct adjacency is often impractical, but proximity still plays a key role in control or influence. The paper also examines the challenges of secure domination within non-cyclic abelian groups and various network topologies, which are commonly represented as graphs.

Many types of dominance criteria have been studied by placing different constraints on dominant sets [5]. Parameters characterisethe most innovative dominance is the quantity of vertices over which a vertex is dominant. Additionally, a study of the dominance polynomial of a particular graph is presented in [6]. The degree of v represented as deg(v), represents the cardinality of G.Numerous studies have been conducted in several domains, including linear algebra, Laplacian, and distance matrices [7–12]. This paper computes new domination results in graphs using a technique called secure distance matrix domination. A few dominating set theorems for secure distance matrices are described.

The lowest cardinality associated with secure overpowering $D_{SDM}\, G$ equal to secure dominance number $\gamma_S D_{SDM}\, (G)$. Cockayne et al. [13] introduced secure domination, which is examined, for instance, in [14–17].

This paper presents a novel approach that integrates advanced cryptographic techniques, privacy-preserving mechanisms, and decentralized control to secure distance matrix domination. Recent advances in homomorphic encryption and secure multi-party computation (MPC) have shown promise in allowing secure computations on encrypted data without revealing the original information. These techniques have been successfully applied in secure network routing and privacy-preserving data analytics (Chen et al., 2022; Zhang et al., 2023). Moreover, the introduction of graph perturbation methods and differential privacy ensures that the graph's sensitive information is not exposed during computations (Narayanan & Shmatikov, 2021).

2. Preliminaries

Definition 2.1

A subset $D_{SDM}(S) \subseteq VD_{SDM}(G)$ that is referred to as Secure Distance matrix dominat set of G if each vertices $D_{SDM}(v) \in VD_{SDM}(G) \setminus D_{SDM}(G)$there exists$D_{SDM}(u) \in D_{SDM}(S)$ such that$D_{SDM}(uv) \in D_{SDM}(E)$and $D_{SDM}(S) = (D_{SDM}(S) - D_{SDM}(u) \cup D_{SDM}(v)$ is a dominating set and the minimum cardinality of secure distance matrix dominating set is the secure Distance matrix dominating number which is denoted by $\gamma_s D_{SDM}(G)$

Definition 2.2

Consider $D_{SDM}(G) = (V(D_{SDM}), E(D_{SDM}))$ be a normal graph. A secure distance matrix dominating set $D_{SDM}(G)$ is defined a secure distance matrix dominating set if for every set $D_{SDM} V_1 \subseteq D_{SDM} V \setminus D_{SDM}(D)$there is a set that is not empty $D_{SDM} D_1 \subseteq D_{SDM}$ Din a way that generated a subgraph$D_{SDM} < V_1 \cup D_{SDM} D_1 >$Resulting from$D_{SDM} V_1 \cup D_{SDM} D_1$ has a connection. The cardinality minimum of secure Distance matrix dominating set is called the secure Distance matrix domination number of $D_{SDM}(G)$and is denoted by $\gamma_s D_{SDM}(G)$.

Definition 2.3

The upper secure distance matrix dominating number, represented by $\gamma_s D_{SDM}(G)$, is the cardinality maximum of a minimal secure distance matrix dominating set of $D_{SDM}(G)$. It is obvious that a dominating set $D_{SDM}(D)$ is only a secure Distance matrix dominating set if and when the set $D_{SDM}(D)$ itself is a secure distance matrix dominating set.

Definition 2.4

A line graph is formed by $D_{SDM}(G) = (V(D_{SDM}), E(D_{SDM}))$, when the set of edges is represented by $E(D_{SDM})$ as well as the one that powers the set of points is implied from $(V(D_{SDM})$. Each of the edge, usually referred to as simply vivj, consists of an unorganized established of two unique vertices, $\{(v_i(D_{SDM}), (v_j(D_{SDM})\}$for $1 \leq D_{SDM}(i) \neq D_{SDM}(j) \leq n$. If there is a path from u to v for every $u, v \in V D_{SDM}(G)$, then graph $D_{SDM}(G)$ is connected.

Definition 2.5

Given an asymmetrical graph $D_{SDM}(G)$ on its vertex set $\{v_1, v_2, \ldots, v_\rho\}$, the $p \times p$ matrix is the Secure Distance matrix an $D_{SDM}(G)$.

$$D_{SDM}(G) = \begin{cases} d(x,y) & \text{if } v_x \leftrightarrow v_y, \\ 0 \quad , & \text{otherwise.} \end{cases}$$

Example 2.5.1[26]

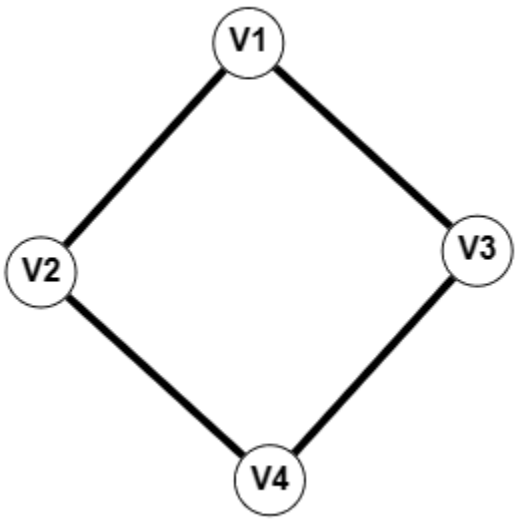


Figure 1: Connected Graph

$$D_{SDM}(G)K_4 = \begin{vmatrix} 0 & 1 & 1 & 2 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 2 & 1 & 1 & 0 \end{vmatrix}$$

Example 2.5.2[26]

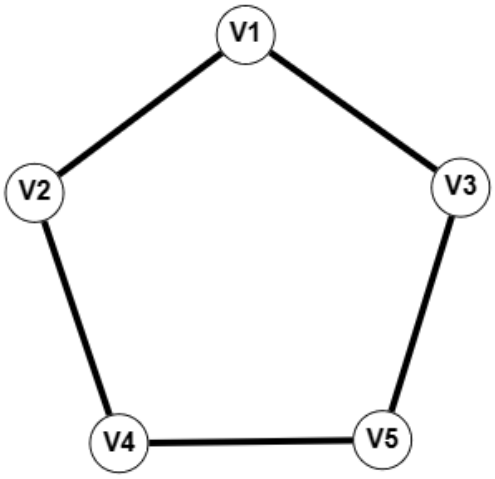


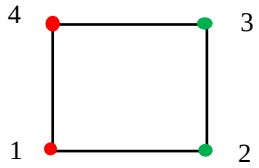
Figure 2: Connected Graph

$$D_{SDM}(G)C_5 = \begin{vmatrix} 0 & 1 & 1 & 2 & 2 \\ 1 & 0 & 2 & 1 & 2 \\ 1 & 2 & 0 & 2 & 1 \\ 2 & 1 & 2 & 0 & 1 \\ 2 & 2 & 1 & 1 & 0 \end{vmatrix}$$

3. Secure Distance Matrix Domination

Example 3.1 [26]

A Set $D_{SDM}(S) = \{1,4\}$.The secure dominant set in graph G. For, $V(D_{SDM}(G)) = \{1,2,3,4\}$.It is the dominant set. $V(D_{SDM}(G) - D_{SDM}(S) = \{2,3\}$. Therefore, Figure 1(b) displays that the D_{SDM} become a secure distance matrix dominating set of $D_{SDM}(G)$.



$$SDM(G) = \begin{matrix} v_2 \\ v_3 \end{matrix} \begin{pmatrix} v_2 & v_3 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$$

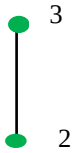


Figure 1(a). Secure dominating set **Figure 1(b).** Secure distance matrix dominating set

Theorem3.2

For the complete graph $K_6, \frac{d}{da}\left(\frac{D_{SDM\ m,n}(K_6,a)}{6}\right) = D_{SDM\ m,n}(K_{6-1}, a) + 1.$

Proof

A Set $D_{SDM}(S) = \{6\}$is the firmly established dominant set. For, $VD_{SDM} = \{1,2,3,4,5,6\}$become a dominating set. $VD_{SDM} - D_{SDM}(S) = \{1,2,3,4,5\}$.

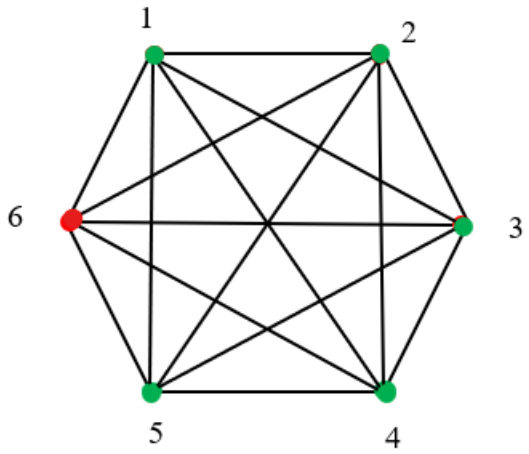


Figure 2(a). Secure dominating set of complete graph K_6

$$\text{SDM (G)} = \begin{matrix} v_1 \\ v_2 \\ v_3 \\ v_4 \\ v_5 \end{matrix} \begin{pmatrix} v_1 & v_2 & v_3 & v_4 & v_5 \\ 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

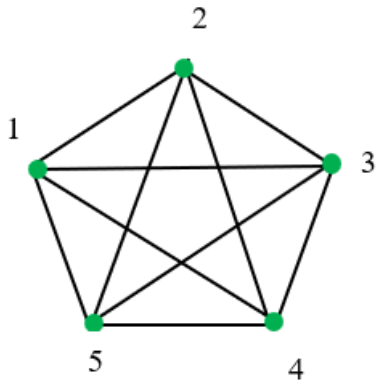


Figure 2(b). Secure distance matrix dominating set of complete graphK_5

We have $D_{SDM\ m,n}(K_6, a) = (1 + a)^6 - 1$.

Therefore, $\frac{d}{da}\left(D_{SDM\ m,n}(K_6, a)\right) = 6(1 + a)^{6-1}$

$$\frac{d}{da}\left(\frac{d(v_m, v_n)(K_6, a)}{6}\right) = (1 + a)^5$$

$$\frac{d}{da}\left(\frac{d(v_m, v_n)(K_6, a)}{6}\right) - 1 = (1 + a)^5 - 1$$

$$= d(v_m, v_n)(K_5, a)$$

Hence,

$\frac{d}{da}\left(\frac{D_{SDM\ m,n}(K_6,a)}{6}\right) = SDM_{m,n}(K_5, a) + 1.$

Theorem3.3

Let D_{SDM} be the secure distance matrix such thatD_{SDM} $S \subseteq V(G)$ and let K_n become a complete graph having D_{SDM} n nodes. Following that, given an algebraic multiplicity of $n - 1$, the eigenvalues of D_{SDM} are $n - 1$ and -1.

Proof

Initially, we demonstrate that -1 is an D_{SDM} eigenvalue by taking into account$D_{SDM\ m,n} = d(v_m, v_n)$, clearly

$$(D_{SDM} - (-1)I_n) = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 1 & 1 & \dots & 1 \end{pmatrix}$$

The other eigenvalue of D_{SDM} is found in the second part of the proof, which assumes thatThe total amount of each and every their eigenvalue in D_{SDM} has become equivalent to the process of tracing.
Given the standing of$(D_{SDM} - (-1)I_n)$ is 1, this implies that $\det(D_{SDM} - (-1)I_n) = 0$ and that negative One of the eigenvalues ofD_{SDM} with algebraic variance of $n - 1$ indexed by $D_{SDM}\, S \subseteq VD_{SDM}(G)$.

$$\begin{aligned} e* + \sum_{i=1}^{n*-1} (-1) &= 0 \\ e* - (n* - 1) &= 0 \\ e* &= (n* - 1). \end{aligned}$$

As result, D_{SDM} 's eigenvalues are $n* - 1$ and -1, with $n* - 1$ algebraic multiplicity.

Theorem3.4
Assume that $D_{SDM}(G)$ is going on secure distance matrix for alinegraph$D_{SDM}\, G$ with $n \geq 2$ vertices that is implies that $D_{SDM}\, S \subseteq D_{SDM}\, V(G)$. With $n* - 1$ negative eigenvalues and one positive eigenvalue, $D_{SDM}(G)$ is then described.
Proof
Using the induction approach on the number of vertices $(n*)$, we shall demonstrate this. Starting there is only one straightforward graph with two vertices when $(n*) = 2$.

$$SDM(G) = \begin{matrix} \\ v_1 \\ v_2 \end{matrix} \begin{pmatrix} v_1 & v_2 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$$

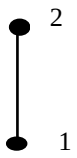


Figure 3. Secure distance matrix dominating set

Let Simple Graph beand Secure distance matrix be$D_{SDM}(G)$.
We calculate the eigenvalues of $SDM(G)$, and we refer to $D_{SDM}(G)$ as D_{SDM} to keep things simple.
Next, we solve,

$$\begin{aligned} \det(D_{SDM} - \psi I) &= 0, \\ \begin{vmatrix} -\psi & 1 \\ 1 & -\psi \end{vmatrix} &= 0, \\ \psi^2 - 1 &= 0, \\ (\psi + 1)(\psi - 1) &= 0. \end{aligned}$$

As a result, we have one eigenvalue that is positive, $\psi = 1$, and one that is negative, $\psi = -1$.
We now suppose that the theory applies to graphs having $n - 1$ vertices and examine $n > 2$.
By removing a vertex, which we refer to as v_a, or a vertex of degree one, from D_{SDM}, we create a subgraph (which is once more a graph) with $n - 1$ vertices.
$D_{SDM\, v_a}$ is the secure distance matrix for the generated subgraph.
Keep in consideration that the separations between the remaining vertices don't change if v_a is removed since it is pendant. This indicates that the submatrix of D_{SDM} called $D_{SDM}\, M_{v_a}$ is created by taking out the columns and rows and column that match the point of intersection v_a.
We assume that the eigenvalues of $D_{SDM\, v_a}$ are $\rho_1, \rho_2, \cdots, \rho_{n-1}$ such that ρ_1 is positive and the remaining eigenvalues are negative.
Let us now assume that the D_{SDM} eigenvalues are $\psi_1, \psi_2, \cdots, \psi_n$. Cauchy's Interlacing Theorem may be applied to the Hermitian matrix's eigenvalues.
The introduction informs us that D_{SDM} is Hermitian. After that, we obtain $\psi_1 \geq \rho_1 \geq \psi_2 \geq \rho_2 \geq \cdots \geq \psi_{n-1} \geq \rho_{n-1} \geq \psi_n$ by using the interlacing theorem. We note that ψ_2 might have a positive or negative value. D_{SDM} has two positive eigenvalues if it is positive; if it is negative, D_{SDM} has only one positive eigenvalue. The sign is supported by the The reality that the matrices determinant's consider is proportional to the product of the eigenvaluesof ψ_2.
Hence,

$$\frac{\det \mathbb{D}_{SDM}}{\det \mathbb{D}_{SDM\ v_a}} = \frac{\psi_1 \cdot \psi_2 \cdots \psi_n}{\rho_1 \cdot \rho_2 \cdots \cdot \rho_{n-1}}.$$

The sign of $\frac{\det \mathbb{D}_{SDM}}{\det \mathbb{D}_{SDM\ v_a}}$ relies on the sign of ψ_2, since ψ_1, ρ_1 are positive, ρ_2 is negative, and $\rho_2 \geq \psi_3 \cdots \geq \psi_{n-1} \geq \rho_{n-1} \geq \psi_n$.

By using the determinant of a graph formula, we obtain

$$\begin{aligned}\frac{\det \mathbb{D}_{SDM}}{\det \mathbb{D}_{SDM\ v_a}} &= \frac{(-1)^{n*-1}(n*-1)2^{n*-2}}{(-1)^{n*-1-1}(n*-1-1)2^{n*-1-2}} \\ &= \frac{(n*-1)}{(-1)(n*-2)2^{-1}} \\ &= \frac{-2(n*-1)}{(n*-2)} < 0.\end{aligned}$$

This suggests that SDM has a single positive eigenvalue since ψ_2 is negative.

Theorem 3.5

If a graph G consists of p components $G_1, G_2, \ldots, G_p$, then

$D_{SDM}(G, x) = D_{SDM}(G_1, x) D_{SDM}(G_2, x) \ldots D_{SDM}(G_p, x)$, for any natural number p.

Proof:

When $p = 2, G = G_1 \cup G_2$.

Therefore $D_{SDM}(G, x) = D_{SDM}(G_1, x) D_{SDM}(G_2, x)$.

Hence, $D_{SDM}(G, x) = D_{SDM}(G_1, x) D_{SDM}(G_2, x) \ldots D_{SDM}(G_p, x)$, for any natural number m.

Corollary 3.6

Assume that the null graph, $\bar{K}_n$, has n * vertices.Then $D_{SDM}(\bar{K}_{n*}, x) = x^{n*}$.

Proof:

Since $D_{SDM}(\bar{K}_1, x) = x$, by Theorem 3.6, $D_{SDM}(\bar{K}_{n*}, x) = x^{n*}$.

Theorem 3.7

Given the adjacency matrix A(G), a subset D⊆V(G) is a dominating set if for every vertex v∈V(G) \setminus Dv∈V(G)\D, there exists a vertex u∈Dsuch that $a_{\{uv\}} = 1$, i.e. for each vertex v not in D, at least one vertex u∈Dmust have a direct connection to v, as indicated by the adjacency matrix.

Proof: We show that the existence of a dominating set DDD corresponds to a structural property of the adjacency matrix A(G).Let D⊆V(G)be the set of vertices that we want to check for domination.For each vertex v∈V(G), inspect the corresponding row of the adjacency matrix A(G).If the row corresponding to vertex v has a non-zero entry in a column corresponding to a vertex in D (i.e., $a_{\{uv\}} = 1$), then v is adjacent to a vertex in D, satisfying the domination condition.If all vertices v∈V(G)\Dhave this property, D is a dominating set.Thus, the set D is a dominating set if the rows corresponding to vertices V(G)\Dhave non-zero entries in columns corresponding to D. Hence, the condition for domination is satisfied through matrix operations on A(G).

Theorem 3.8

Let D(G) be the distance matrix of a graph G, where d_{ij} is the shortest path distance between vertices i and j. A subset S⊆V(G)is a distance-dominating set if for every vertex v∈V(G)\S, there exists a vertex u∈Ssuch that $d_{uv} \leq k$ for a given k.

Proof: We aim to prove that this condition can be verified using the distance matrix D(G)Let S⊆V(G)be the set of vertices we are testing for distance domination.For each vertex v∈V(G)\S, inspect the row corresponding to v in the distance matrix D(G).In this row, check whether there is a column corresponding to a vertex u∈Swhere $d_{uv} \leq k$. This would indicate that v is within distance k from a vertex in S.If such a u exists for all v∈V(G)\S, then S is a distance-dominating set.Thus, by examining the distance matrix and checking for entries $d_{uv} \leq k$, we confirm that S is a distance-dominating set if this condition is satisfied for all v∈V(G)\S. The matrix formulation provides a clear method for verifying distance domination.

4. Application of Secure Distance Matrix Domination

4.1 Encryption of Distance Matrices

The core idea here is to securely handle the distance matrix to prevent unauthorized access while ensuring that computations can still be performed. Homomorphic encryption schemes, which allow computations on encrypted data, can be used for this purpose:

Homomorphic Encryption (HE) and Partially Homomorphic Encryption (PHE) enable secure computations on encrypted data. The idea here is that the graph's distance matrix can be encrypted, allowing parties to perform operations like shortest path calculations or dominating set identification without decrypting the matrix.

- **Fully Homomorphic Encryption (FHE):** FHE allows any operation on encrypted data without needing to decrypt it. If the distance matrix is encrypted using FHE, the dominating set or centrality measures can be calculated directly, providing a strong layer of security.
- Use case: In scenarios where the distance matrix represents sensitive relationships, such as in social networks or communication infrastructure, FHE can allow secure computation of network centrality or domination without revealing actual distances.
- **Partially Homomorphic Encryption (PHE):** This is simpler and faster than FHE but only allows specific operations like addition or multiplication. PHE can be sufficient if only limited operations on the distance matrix (e.g., simple path length computations) are needed.
- Use case: Secure routing in network traffic, where certain operations are sufficient for determining optimal paths while maintaining security.

4.2 Secure Multi-party Computation (MPC)

In scenarios where multiple parties collaborate on graph-related problems without revealing their individual data, Secure Multi-party Computation can enable a group of participants to jointly compute the distance matrix or perform domination functions without exposing their individual nodes or edges. This enhances privacy and ensures no single party has full control over the data.

In MPC, multiple parties collaborate on a computation while keeping their inputs private. Applied to distance matrix domination, this allows several nodes (or stakeholders) to jointly compute the domination set or other properties without sharing the entire graph structure.

- **Implementation:**
  - Each party holds part of the graph data (edges, nodes, etc.), and they collaborate using cryptographic protocols to jointly compute the dominating set or perform distance matrix-related calculations.
  - The individual distance submatrices can be computed privately, and the overall result is securely aggregated.
- **Use case:** Secure multi-party graph computation is useful when different organizations need to collaborate without revealing proprietary or sensitive network structures, such as in distributed logistics or supply chain networks.

4.3 Graph Perturbation Techniques

To protect the structure of the graph from potential attackers, perturbing the graph's structure (e.g., adding random edges or modifying weights) while preserving the essential properties of the distance matrix is a powerful technique. Differential privacy could be applied to ensure that the information revealed through the distance matrix does not compromise the original graph’s privacy.

Graph perturbation involves making slight changes to the graph's structure (such as adding/removing edges or modifying weights) in order to protect sensitive information about its nodes and edges. Differential Privacy (DP) is a formal framework that ensures these perturbations do not reveal too much about individual nodes or connections.

- **Differentially Private Graph Algorithms:**
  - DP mechanisms can be applied to compute an approximate distance matrix where slight noise is added to distances. This protects the underlying structure while allowing domination or centrality calculations.
  - Another approach involves adding or removing edges randomly to mask key connections between nodes without significantly altering the graph's overall properties.
- **Use case:** In social network analysis, DP could protect individuals' privacy while allowing researchers to study dominant communities or highly influential nodes without revealing specific relationships.

4.4 Randomized Shortest Path Computations

Instead of computing deterministic shortest paths, randomized algorithms can be used to introduce variability into the results. This masks the exact structure of the graph and prevents an attacker from reverse-engineering the network topology.

- **Method:**
  - Shortest path calculations can be randomized by introducing slight variations (e.g., random delays or noise in edge weights) to the distance matrix. The dominating set can then be computed on the randomized matrix, providing enough accuracy for domination but obfuscating the true paths.
- **Use case:** In communication networks or transport systems, randomized path computations make it difficult for adversaries to predict routes or identify central nodes.

4.5 Zero-Knowledge Proofs (ZKP) for Verification

Zero-Knowledge Proofs allow one party to prove that a computation (such as determining the dominating set) was done correctly, without revealing the underlying data. This ensures both privacy and correctness in domination tasks.

- **Implementation:**
  - ZKPs can be applied to verify that a distance matrix is correctly computed, or that a dominating set was correctly identified, without revealing the actual node distances or graph structure.
  - The prover can demonstrate knowledge of a valid dominating set while keeping the set and the graph structure hidden from the verifier.
- **Use case:** ZKP is especially useful in scenarios where correctness needs to be verified by third parties, such as in secure voting systems or blockchain-based consensus networks, where the graph represents stakeholders' positions.

4.6 Decentralized Control and Domination

Decentralization distributes control of the graph and its domination calculations across multiple nodes, rather than relying on a central authority. Technologies like blockchain can ensure that the domination process is tamper-proof and secure.

- **Method:**
  - A decentralized algorithm could involve distributing the domination task across nodes in the network, with consensus mechanisms ensuring that no single node has control over the domination process.
  - Blockchain-based systems can be used to ensure the integrity of the domination results by immutably recording the outcomes of graph computations.
- **Use case:** In decentralized networks like peer-to-peer systems, decentralized control prevents any single node from gaining undue influence over routing or resource allocation.

4.7 AI and Machine Learning for Anomaly Detection

Artificial intelligence (AI) and machine learning (ML) models can be used to monitor graph domination processes, detecting anomalies or suspicious changes in the graph structure that could indicate attacks.

- **Implementation:**
  - Graph-based ML algorithms can learn typical patterns in the distance matrix and recognize anomalies that may indicate attempts to manipulate or attack the graph.
  - AI can help optimize the domination process itself, learning which nodes are likely to be critical for control based on historical data.
- **Use case:** In network security, AI could be used to detect changes in domination metrics that might indicate intrusion or tampering with the graph's topology.

4.8 Quantum Cryptography for Enhanced Security

Quantum cryptography provides future-proof security measures against threats posed by quantum computing, which could break classical encryption methods. In the context of graph domination, **Quantum Key Distribution (QKD)** could be used to securely share information about the graph or its distance matrix.

- **Method:**

- QKD ensures that keys used to encrypt the distance matrix or other graph data cannot be intercepted or broken by quantum computers.
- Post-quantum cryptographic algorithms can also be used to protect the graph data from future attacks.

- **Use case:** In highly sensitive applications such as government networks or critical infrastructure, quantum cryptography ensures that the domination process remains secure even in the face of advanced future technologies.

5. Conclusion and Future works

The novel approach to secure distance matrix domination in fundamental graphs combines multiple advanced cryptographic, computational, and privacy-preserving techniques to enhance the security, privacy, and efficiency of domination tasks. Through the use of encryption (Homomorphic and Partially Homomorphic), Secure Multi-party Computation (MPC), graph perturbation with Differential Privacy, and randomized algorithms, sensitive graph data can be protected while still enabling essential operations such as shortest path computations and domination set identification.Incorporating Zero-Knowledge Proofs (ZKP) ensures the correctness of results without revealing underlying graph structures, while decentralized control mechanisms (like blockchain) eliminate the risks associated with centralization, ensuring integrity and robustness. Furthermore, machine learning techniques can monitor domination processes to detect anomalies, and quantum cryptography offers future-proof security against emerging quantum threats.This comprehensive approach makes it possible to securely dominate nodes in a variety of practical applications—such as network routing, social network analysis, and distributed computing—without compromising the privacy or security of the underlying graph structure. It provides a blueprint for the future of secure computations on graphs, where privacy, scalability, and resistance to attack are essential.

REFERENCES

[1] P. J. Campbell, Gauss and the eight queens problem: A study in miniature of the propagation of historical error. Historia mathematica, 4(4), 397-404 (1977).
[2] O. Ore, Theory of Graphs, American Mathematical Society, Provedence, R.I, (1962).
[3] F. Harary, Graph Theory, Addison- Wesley, Reading Mass, (1969).
[4] M. S. Rahman, Basic Graph Theory, Springer, India, (2017).
[5] T. W. Haynes and S.T. Hedetniemi, P. J. Slater, Fundamentals of domination in graphs, Marcel Dekker, Inc., New York, (1998).
[6] R.B. Bapat, Determinant of the distance matrix of a tree with matrix weights, Linear Algebra Appl. 416, 2–7 (2006).
[7] R.B. Bapat, S.J. Kirkland, M. Neumann, On distance matrices and Laplacians, Linear Algebra Appl. 401, 193–209 (2005).
[8] R.B. Bapat, A.K. Lal, S. Pati, A q-analogue of the distance matrix of a tree, Linear Algebra Appl. 416, 799–814 (2006).
[9] M. Edelberg, M.R. Garey, R.L. Graham, On the distance matrix of a tree, Discrete Math. 14, 23–39 (1976).
[10] M. Fiedler, Algebraic connectivity of graphs, Czechoslovak Math. J. 23(98), 298–305 (1973).
[11] P.W. Fowler, G. Caporossi, P. Hansen, Distance matrices, wiener indices, and related invariants of fullerenes, J. Phys. Chem. A 105, 6232–6242 (2001).
[12] R.L. Graham, L. Lovász, Distance matrix polynomials of trees, Adv. Math. 29, 60–88 (1978).
[13] E.J. Cockayne, P.J.P. Grobler, W.R. Grundlingh, J. Munganga, J.H. van Vuuren, Protection of a graph, Util. Math. 67 (2005) 19–32. 790
[14] W.F. Klostermeyer, C.M. Mynhardt, Secure domination and secure total domination in graphs, Discuss. Math., Graph Theory 28 (2008) 267–284.
[15] C.M. Mynhardt, H.C. Swart, L. Ungerer, Excellent trees and secure domination, Util. Math. 67 (2005) 255–267.
[16] E. J. Cockayne, Irredundance, secure domination and maximum degree in trees, Discrete Math., 307 (2007), 12–17.
[17] Merouane, H. B., & Chellali, M. (2015). On secure domination in graphs. Information Processing Letters, 115(10), 786-790.
[18] A. Hansberg, D. Meierling and L. Volkmann, Distance Domination and Distance Irredundance in Graphs, Elec. J. Combin. (2007), R35.
[19] J.H. Hattingh and M. A. Henning, The ratio of the distance irredundance and domination numbers of a graph, J. Graph Theory 18 (1994), 1-9.

[20] S. G. Li, On connected k-domination numbers of graphs, Discrete Math. 274 (2004), 303-310.
[21] D. Rautenbach and L. Volkmann, On $\alpha_r\gamma_s$(k)-perfect graphs, Discrete Math. 270 (2003), 241-250.
[22] Tian, F., & Xu, J. M. (2009). A note on distance domination numbers of graphs. Australas. J Comb., 43, 181-190.
[23] Arora, A., Dey, H. K., & Goel, S. (2023). Distance matrix of enhanced power graphs of finite groups. arXiv preprint arXiv:2304.04288.
[24] R.L. Graham, H.O. Pollack, On the addressing problem for loop switching, Bell System Tech. J. 50 (1971) 2495–2519.
[25] M. Edelberg, M.R. Garey, R.L. Graham, On the distance matrix of a tree, Discrete Math. 14 (1976) 23–39
[26] Neethialagan, M.G. and Meenakshi, S., 2024. Secure Distance Matrix Domination Graphs. Journal of Electrical Systems, 20(7s), pp.2437-2452.
[27] R.L. Graham, L. Lovász, Distance matrix polynomials of trees, Adv. Math. 29 (1978) 60–88.
[28] C. M. Jones, Security and secure-dominating sets in graphs (Doctoral dissertation, Auburn University) (2014).
[29] Randy Davila, Caleb Fast, Michael A. Henning and Franklin Kenter, Lower Bounds on the Distance Domination Number of a Graph, arXiv:1507.08745v1 [math.co], 31 (2015).
[30] Risan Nur Santi, IkaHesti Agustin, Dafik, Ridho Alfarisi, On the locating domination number of corona product, IOP Conf. Series: Journal of Physics: Conf. Series, 1008 (2018), 12–53.
[31] D.P. Salve, E.L. Enriquez, Inverse Perfect Domination in the Composition and Cartesian Product of Graphs, Global Journal of Pure and Applied Mathematics, 2(1) (2016), 1–10.
[32] Santiago Canales, Gregorio Herna´ndezb, Mafalda Martins and Ineˆs Matosc, Distance domination, guarding and covering of maximal outerplanar graphs, Discrete Applied Mathematics, 181 (2015), 41–49.
[33] D.A.R. Wardani, Dak, I.H. Agustin, E.Y. Kurniawati, On Locating Independent Domination Number of Amalgamation Graphs, IOP Conf. Series: Journal of Physics: Conf. Series, 943 (2017), 12–27.
[34] Lars Jaffke, joungkwon, Torstein J.F.Strmme, Jan Arne Telle, Mim-width III. Graph powers and generalized distance domination problems , Theoretical Computer Science ,796 (2019) 216–236.
[35] Canan Ciftci, Disjunctive Total Domination of Some Shadow Distance Graphs , Fundamental Journal of Mathematics and Applications , 3(2) (2020) 185–193.
[36] E.L. Enriquez, Super Fair Dominating Set in Graphs, Journal of Global Research in Mathematical Archives, 6(2) (2019), 8–14.
[37] E.L. Enriquez , G.T. Gemina, Super Fair Domination in the Corona and Lexicographic Product of Graph, International Journal of Mathematics Trends and Technology, 66(4) (2020), 203–210.
[38] E.L. Enriquez and S.R. Canoy, Jr. Secure Convex Domination in a Graph, International Journal of Mathematical Analysis, 9(7) (2015), 317–325.
[39] E.L. Enriquez, and S.R. Canoy, Jr., Secure Convex Domination in a Graph, International Journal of Mathematical Analysis, 9(7) (2015), 317–325.
[40] G.M. Estrada, C.M. Loquias, E.L. Enriquez and C.S. Baraca, Perfect Doubly Connected Domination in the Join and Corona of Graphs, International Journal of Latest Engineering Research and Applications, 4(7) (2019), 17–21.