JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES
www.journalimcms.org

ISSN (Online) : 2454 -7190 Vol.-20, No.-6, June (2025) pp 51 - 64 ISSN (Print) 0973-8975

SECURE VERTEX-EDGE DOMINATION IN HYPERCUBE AND GRID GRAPHS: APPLICATIONS OF CYBERSECURITY IN BANKING FOR SECURE TRANSACTIONS

C. Ruby Sharmila[1], S. Meenakshi[2]

[1,2] Department of Mathematics, Vels Institute of Science Technology and Advanced Studies, Pallavaram, Chennai, Tamil Nadu 600117, India.

Email: [1]sharmi.ruby2011@gmail.com, [2]meenakshikarthikeyan@yahoo.co.in

Corresponding Author: **C. Ruby Sharmila**

https://doi.org/10.26782/jmcms.2025.06.00004

(Received: December 02, 2024; Revised: April 29, 2025; Accepted: May 16, 2025)

Abstract

In the banking sector, safeguarding sensitive financial transactions is critical to maintaining customer trust and regulatory compliance. Cybersecurity threats, ranging from data breaches to unauthorized access, necessitate robust protective measures. However, the majority of research places a strong emphasis on vertex dominance in security networks while ignoring the importance of edge defense for overall security, also hypercube and grid structures are not considered. Furthermore, conventional studies have ignored the potential of hypercube and grid graph structures in enhancing security measures. Hence this research proposed a secure vertex-edge domination (SVED) in hypercube and grid graphs, exploring their applications in optimizing cybersecurity measures for secure transaction monitoring. Moreover, develop a Hidden Markov Model (HMM) framework to enhance the detection of anomalous activities within these graph structures. This algorithm efficiently computes the minimum number of security agents required to monitor transaction flows, thus reducing vulnerabilities. This research not only fills a critical gap in existing network security methodologies but also proposes a novel framework for protecting complex networks from evolving cyber threats, thereby advancing the frontier of cybersecurity and mathematical graph theory.

Keywords: Secure Vertex-Edge Domination, Hypercube graphs, Grid graphs, Graph theory, Cybersecurity threats, Secure Transaction

I. Introduction

Digital banking becoming a norm in modern-day banking systems, and financial institutions must secure the transaction process. The rapid proliferation of online and mobile banking services has opened an exponentially larger attack surface for cybercriminals. Cyber threats have evolved in targeting banking infrastructures from traditional risks, such as phishing and unauthorized access, to more advanced techniques, including man-in-the-middle attacks, malware, and ransomware. These

attacks not only undermine individual accounts but also pose an ever greater threat to the system in general. With such interconnectivity of many nodes, including ATMs, point-of-sale, internet banking, and mobile banking, transaction monitoring has been brought to the forefront as an extremely critical function. While requiring real-time processing, transactions must also be securely maintained with the sensitive assets of customers. With such heightened risks, there are strong measures of cybersecurity that have surfaced to actively detect, prevent, and mitigate fraud activities [Angel, Uma, et al., (2023, October); Alzoubi, Ghazal, et al.,(2022 May); Majeed and Rauf, (2020)].

The architecture of modern banking networks presents unique challenges for transaction security. Unlike centralized systems, where a single point of failure can be defended using traditional security measures, the distributed nature of banking infrastructures requires more advanced, multi-layered security strategies. Each node in the network, whether it is an ATM, a digital wallet, or an online banking interface represents a potential vulnerability. To safeguard against cyber threats, security frameworks must protect both the transaction endpoints and the connections that link them. This requires a more dynamic approach, combining real-time monitoring, anomaly detection, encryption, and access control mechanisms to secure the entire financial ecosystem [Zhang, Wang, et al.,(2023 November); Stanikzai, Shah, (2021 December)]. A particularly promising approach to securing banking transactions is the use of advanced graph-theoretic techniques. By modeling the banking network as a graph, with nodes representing transaction points and edges representing communication links, graph theory allows for deeper analysis of vulnerabilities. One specific area of focus is on SVED, a concept that provides insights into the strategic placement of cybersecurity measures, such as firewalls, intrusion detection systems, and transaction monitoring algorithms, to ensure comprehensive protection. SVED aims to not only monitor and control each node in the network but also ensure the security of the communication channels between nodes, thereby creating multiple layers of defense against cyberattacks [Zhang, Liu, (2020 March); Al-Alawi, and Al-Bassam, (2020)].

I.i Background

While traditional cybersecurity strategies in banking have concentrated on securing individual devices and databases, the broader challenge lies in securing both the vertices (transaction points) and the edges (data transmission paths) in the network. This dual focus ensures that even if a single node or connection is compromised, there are redundancies and backups in place to maintain transaction integrity. Moreover, as banking institutions continue to evolve and adopt cloud-based solutions, peer-to-peer payment systems, and other digital innovations, the need for scalable, secure monitoring mechanisms becomes increasingly crucial. Despite the advances in transaction monitoring and cybersecurity, there remain gaps in the application of graph theory, particularly in the context of various models [Wang, Zhang, et al.,(2021); Chelvam, and Sivagami, (2021)]. These graph structures, which are vital for representing complex, multidimensional transaction networks, have yet to be fully explored in terms of their potential to enhance security in banking. Hypercube graphs, with their high scalability and efficiency, are especially relevant for multi-channel banking systems that handle vast amounts of data in real-time. Similarly, grid graphs,

commonly used in sensor networks and geographical applications, provide new perspectives on monitoring and securing distributed banking infrastructures [Kulli, (2016); Boutrig, Chellali, et al.,(2016); Sahin, and Sahin, (2020); DeVivo, Hladky, (2024); Angel, Arputhamary, et al.,(2021 February); Golubev, (2020)].

Dumitrescu et al. [Dumitrescu, Băltoiu, et al.,(2022)] highlight the importance of detecting bank clients involved in suspicious activities through transaction graphs, employing innovative features derived from reduced egonets and random walks to enhance anomaly detection. Similarly, Wang and Zhu [Wang, Zhu, (2022)] propose a graph-based behavioral identification paradigm that integrates property-level associations into behavioral modeling, demonstrating the versatility of graph theory in addressing cybersecurity challenges across various domains. The lack of comprehensive studies on SVED in these graph models presents an opportunity for further research. By extending domination strategies to protect both nodes and edges in banking networks, cybersecurity frameworks are strengthened to guard against sophisticated threats, ensuring that digital transactions remain secure and fraud is swiftly detected and mitigated.

I.ii. Objective of this research

The objective of this paper is as follows.

- To design a new cybersecurity framework that employs Secure Vertex-Edge Domination (SVED) on hypercube and grid graphs to enhance secure transaction monitoring in banking systems.

This research will bridge the gap between theoretical graph-based security models and practical banking applications, providing financial institutions with an effective toolset to defend their transactions against cyber threats. The paper's content is planned as follows: The preliminaries are shown in section 2, the proposed solution and theorems are given in section 3, applications of the proposed algorithm are given in section 4, and the paper is concluded in section 5.

II. Preliminaries

This section defines the most important terms and concepts used in graph-based representations, particularly directed toward the study of SVED in Hypercube and Grid Graphs.

The Graph

A graph $G = (U, F)$ is a mathematical structure used to model pairwise relationships between objects. The set U consists of vertices (or nodes), and F consists of edges, which represent connections between pairs of vertices. An edge $e = \{v, w\}$ is said to be incident to vertices v and w. Graphs are widely used to model various types of networks, such as communication networks, transportation systems, and distributed computing systems.

Hypercube Graph

A hypercube graph S_n is an n-dimensional graph where each vertex corresponds to a binary string of length n. Vertices n and v are connected by an edge if and only if their binary strings differ by exactly one bit. The hypercube is highly symmetric and has 2^n vertices and $2^{n-1}n$ edges. Hypercube graphs are commonly used in parallel computing systems and network models due to their balanced structure and high fault tolerance. They are also referred to as n-cubes**.**

Grid Graph

A grid graph $M_{a,b}$ is a graph whose vertices correspond to points in a two-dimensional lattice of size $a \times b$, where a and b are the numbers of rows and columns, respectively. Each vertex in the grid graph is connected to its immediate neighbors, forming a mesh-like structure. Grid graphs are widely used to model physical layouts, sensor networks, and distributed systems. They consist of ab vertices and typically $2ab - a - b$ edges (for interior points connected to four neighbors, and fewer for edge points). Grid graphs are commonly used to model two-dimensional network topologies, such as sensor grids and urban networks.

Domination Set

A dominating set $D \subseteq U$ of a graph G is a subset of vertices such that every vertex $v \in U \setminus D$ is adjacent to at least one vertex $v \in D$. In other words, all vertices in G are either in D or are neighbors of vertices in D. The domination number $\gamma(G)$ is the minimum size of such a dominating set. The domination concept is widely used in resource optimization problems, where certain nodes (vertices) must control or cover the network efficiently.

Secure Domination

Assume that the basic graph G has order n. If each vertex in $U - H$ is next to a vertex in H, then $\{H\} \subseteq U$ is a dominant set of G. Graph G shows a stable dominating set H is a dominant set with the characteristic of being next to each vertex $v \in (v - H)$ so that $(H - \{v\}) \cup (\{w\})$ is a dominating set. The secure domination number, represented by $\gamma_s(G)$, is the minimal cardinality of a secure dominating set of G.

Secure Vertex-Edge Domination

A dominating set $\{S_{ev}\} \subseteq U(G)$ of a graph G is said to be an SVED set of G if, for all edges, then there exists a vertex $y \in \{S_{ev}\}$ such that y defends the edge e. That is, a vertex in $\{S_{ev}\}$ defends the edges incident on that vertex and the edges which are adjacent to that incident edges. A SVED set $\{S_{ev}\}$ of a graph G is a dominating set with the property that each vertex $z \in U - \{S_{ev}\}$ is either adjacent to a vertex or a vertex adjacent to the incident edges of $z, y \in \{S_{ev}\}$ such that $(\{S_{ev}\} - \{y\}) \cup (\{z\})$ is a dominating set. The SVED Number, denoted by $\gamma_{se}(G)$, is the minimum number of vertices in an SVEDS for the graph G.

III. Proposed work

This section presents the concept of SVED in the context of hypercube and grid graphs, with applications aimed at enhancing cybersecurity in banking systems for secure transaction monitoring. The following Figure 1 illustrates the network of the banking transaction system.

Fig. 1. Network of banking transaction system

As banking infrastructures become increasingly trusting to process financial transactions, protecting these systems from cyber threats is important. SVED offers a comprehensive security framework, ensuring that both the transaction nodes (e.g., ATMs, banking servers, user devices) and the communication links between them are safeguarded. This study explores the secure domination number for n-dimensional hypercubes and grid graphs, establishing a mathematical framework to optimize the allocation of security resources, such as encryption systems and intrusion detection mechanisms, for secure financial transactions.

Secure Vertex-Edge Domination in Hypercube Graphs

This section describes the definition of SVED on hypercube graphs as it relates to a very important factor concerning enhancing security in banking against cyber threats. Hypercube graphs, due to their high dimensionality and scalability, serve as a powerful model for banking systems that require robust security across multiple transaction channels. This concept ensures that not only are the vertices (representing transaction nodes) adequately monitored, but that each selected vertex is also supported by at least one adjacent vertex, thereby providing redundancy and enhancing the reliability of transaction validation. This section presents a formal definition and theorem related to SVED in hypercube graphs, followed by proof establishing its significance in securing transaction nodes and safeguarding the integrity of financial operations. The Hypercube Graph is shown in the following Figure 2.

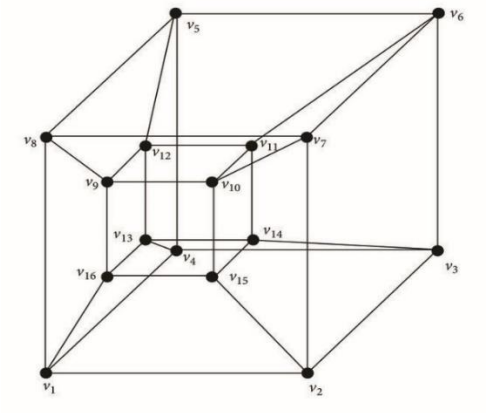

Fig. 2. Hypercube Graph

Theorem 3.1:

For an n-dimensional hypercube S_n, the SVED number $\gamma_{se}(S_n)$, is given by:

$\gamma_{se}(S_n) = 2^{n-1}$

Proof :

Let $G = S_n$ be the hypercube with 2^n vertices and the number of edges of the hypercube graph is given by $2^{n-1}n$. To secure the edges of S_n, need to identify a subset of vertices (transaction nodes) that monitors all edges while ensuring that each selected vertex is supported by at least one adjacent vertex. This promises that each transaction is validated by its neighboring nodes, providing redundancy and enhancing security. The dominating set must thus cover both direct edge connections and ensure redundancy through neighboring vertices.

To prove this theorem, mathematical induction is used for any n-dimensional hypercube:

Base Case ($n = 1$): For a 1-cube (a single edge), the secure domination number is $\gamma_{se}(S_1) = 2^{1-1} = 1$. This holds.

To prove the result for any n: Assuming for $n = k$,

$$\gamma_{se}(S_k) = 2^{k-1} \qquad \text{for } n = k + 1$$

This means for the k-dimensional hypercube, there exists an SVED set with a size 2^{k-1}. We need to prove that $\gamma_{se}(S_{k+1}) = 2^k$.

The n-dimensional hypercube S_{k+1} is constructed as two copies of S_k with corresponding vertices in the two subgraphs connected by an edge. By the induction hypothesis, each S_k has an SVED set of size 2^{k-1}. To extend this to S_{k+1}, we need to ensure that the dominating set for the additional edges connecting the two copies of S_k also satisfies the security condition. A SVED set for S_{k+1} is constructed by taking two secure dominating sets from each S_k subgraph, ensuring that all vertices and connecting edges are securely dominated. Thus, the total number of secure vertices needed for S_{k+1} is:

$\gamma_{se}(S_{k+1}) = 2^{(k+1)-1} = 2^k$.

Therefore, by the principle of mathematical induction conclude that, for any n-dimensional hypercube SVED for S_n is,

$\gamma_{se}(S_n) = 2^{n-1}$ for all $n \geq 1$

In practical applications, implementing SVED in hypercube-based banking networks allows financial institutions to mitigate vulnerabilities, ensuring comprehensive monitoring and robust protection against cyber threats. The integration of SVED in hypercube graphs into HMM for secure transaction monitoring establishes a robust framework that enhances the security of banking transactions. By providing a systematic approach to validate transactions through a dominant set of vertices, this method addresses the increasing challenges posed by cybersecurity threats in the financial sector.

The HMM serves as a crucial algorithm in this approach to optimizing cybersecurity through SVED. The HMM is particularly effective for modeling sequences of observed data where the underlying system is not directly visible, which aligns well with the nature of banking transactions.

Algorithm 3.1: SVED of S_n, Algorithm

Input: An n-dimensional hypercube graph S_n

Output: A SVED set S_{ev} for S_n

1. Initialization:

Define the hypercube graph S_n based on the number of transaction nodes.

Set $S_{ev} = \emptyset$.

$V = \{v_1, v_2, \dots, v_n\}$(Set of vertices in S_n)

$E = \{e1, e2, \dots, en \cdot 2(n-1)\}$ (Set of edges in S_n)

HMM parameters: States, observations, transition probabilities, emission probabilities.

2. Vertex Selection

For each vertex $v_i \in V$

a. Use HMM to determine the chance of v_i being part of the secure dominating set based on transaction history.

b. If v_i is a transaction node, add it to S_{ev}

For each $v_i \in S_{ev}$

Identify adjacent vertices $A(v_i)$such that $A(v_i) = \{v_j \in V | (v_i, v_j) \in E\}$

Ensure that for each edge $((v_i, v_j)$ either v_i or v_j is included in S_{ev} based on their HMM probabilities.

---

3. Ensure complete edge coverage

For each edge $e \in E$

If e is not dominated by any vertex in S_{ev}:

Select an appropriate vertex from $A(v_i)$ based on HMM output and add it to S_{ev} to ensure coverage.

Continuously monitor transaction patterns using the HMM:

Update transition and emission probabilities based on real-time transaction data.

Adapt the SVED set S_{ev}

4. Termination Condition

If all edges in E are dominated

Exit the loop.

5. Return

Return the SVED Set (S_{ev}) and Validated transactions.

Incorporating SVED from hypercube graphs, enhances the robustness of HMMs by ensuring that transaction validations are supported by a secure and redundant network of nodes, represented as vertices in the hypercube graph.

Example 3.1: SVED for S_4

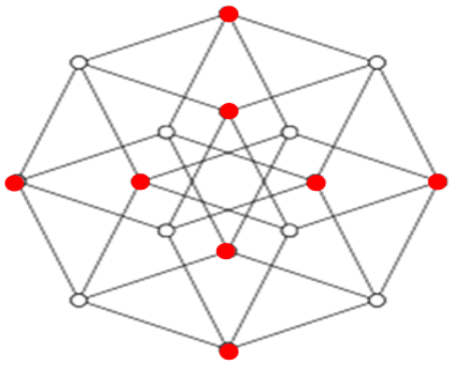

Fig. 3. $\gamma_{se}(S_4) = 8$

The 4-dimensional hypercube S_4 has 16 vertices and 32 edges, which is shown in Figure 3. According to the formula:

$$\gamma_{se}(S_4) = 2^{4-1} = 2^3 = 8$$

Thus, 8 critical nodes are required to securely dominate the entire network, ensuring that every communication link between transaction endpoints is protected. This level of efficiency in security resource allocation is particularly beneficial for high-dimensional banking systems that handle large volumes of transactions across multiple channels.

Secure Vertex-Edge Domination in Grid Graphs

Grid graphs are a suitable framework for implementing strong monitoring strategies due to their structured connectivity and predictable routing paths. SVED enhances the threat detection and resource allocation process by optimizing the choice of vertices and edges for surveillance. This will ensure continuous monitoring of all financial transactions and minimize vulnerabilities while strengthening the overall security architecture of banking networks. Figure 4 shows the structure of the grid graph.

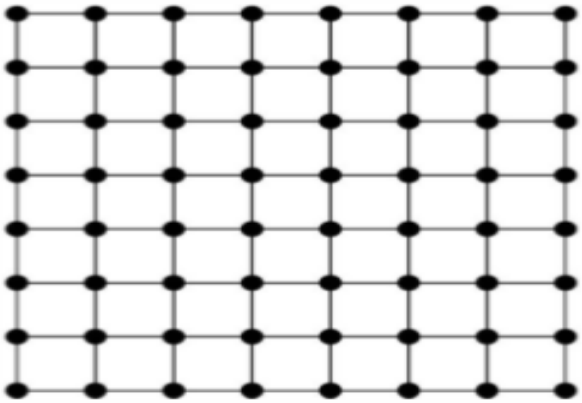

Fig. 4. Grid graph of ($M_{8,8}$)

Theorem 3.2:

Let $M_{a,b}$ be a grid graph where a is the number of rows and b is the number of columns. The SVED number $\gamma_{se}(M_{a,b})$ is the smallest amount of vertices required for each edge of a graph to be either incident to a dominated vertex or next to an edge that is incident to a dominated vertex.

$$\gamma_{se}(M_{a,b}) = \begin{cases} \dfrac{ab}{2}, & if\ ab\ is\ even\ and\ a,b \geq 2 \\ \dfrac{ab+1}{2}, & if\ ab\ is\ odd\ and\ a,b \geq 2 \end{cases}$$

Proof:

Case (i): Let ab be even

If ab is even and $a = b = 2$. A possible SVED set is $\{v_{11}, v_{22}\}$, which secures both vertices and all edges incident to them, then the SVED number $\gamma_{se}(M_{2,2}) = 1$

Assume the theorem holds for all $k \times k$ grids where $k \leq a$ and $k \leq b$. Now consider $M_{a,b}$ where a and b are both even. Each selected vertex will dominate its adjacent edges. In a checkerboard pattern, each dominated vertex will cover its four neighboring edges, effectively covering multiple edges with fewer vertices. The total number of vertices in a checkerboard pattern is $\frac{ab}{2}$ because: For an even a and b, there are exactly $\frac{ab}{2}$ dominated vertices. Thus, we conclude that $\gamma_{se}(M_{a,b}) = \frac{ab}{2}$ when ab is even.

Case (ii): Let ab is odd.

Assume the theorem holds for all $k \times k$ grids where $k \leq a$ and $k \leq b$. Now consider $M_{a,b}$ where a, b is odd:

Since ab is odd, let's calculate how many secure vertices are required to cover all vertices optimally: Place secure vertices in a checkerboard pattern to maximize the number of dominated vertices. For each $2x2$ block of the grid, we place two secure vertices to cover four vertices. Similar to the even case, divide the grid into two subgrids, with one additional row and column. Each of the four subgrids requires $\frac{(a-1)(b-1)}{2}$. Consequently, the minimum number of vertices required in the SVEDS to achieve SVED for $M_{a,b}$ When ab is odd is $\gamma_{se}(M_{a,b}) = \frac{ab+1}{2}$.

Therefore, the SVED number of a grid graph $M_{a,b}$ depends on whether the product ab is even or odd. The domination number is $\frac{ab}{2}$ when ab is even, and $\frac{ab+1}{2}$ when ab is odd. The theorem states that the SVED number of a grid varies with the parity of its dimensions a and b. Each case has been proven based on the structure of the grid and the selection of dominators, ensuring coverage of all vertices and edges in $M_{a,b}$.

Example 3.2: SVED for $M_{4,4}$

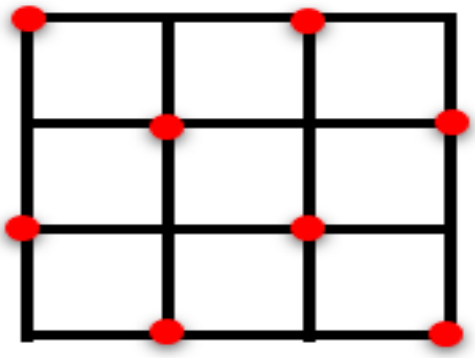

Fig. 5. $\gamma_{se}(M_{4,4}) = 8$

The grid $M_{4,4}$ consists of 4 rows and 4 columns, resulting in a total of 16 vertices and 24 edges, which is shown in Figure 5. To determine the SVED number γ_{se} for this grid, we can apply the theorem 3. According to the theorem:

$$\gamma_{se}(M_{4,4}) = \frac{ab}{2} = \frac{4 \times 4}{2} = \frac{16}{2} = 8$$

This demonstrates that in the grid graph $M_{4,4}$, selecting secure vertices in a checkerboard pattern allows us to dominate all vertices and edges effectively. This configuration ensures that each vertex placed dominates its adjacent edges effectively. Each of the chosen vertices covers its four neighboring edges, thus securing multiple edges with each selected vertex. Therefore, the theorem holds for $M_{4,4}$ and the SVED number is indeed 8. This efficient allocation of secure vertices is important in

enhancing the security of banking networks, ensuring that all transaction pathways are continuously monitored and protected.

To further enhance the effectiveness of the SVED strategy, the HMM framework is introduced. HMMs are statistical models that represent systems with hidden states and continuous values. This concept is applied in modeling dynamic behaviors of vertices and edges, using an HMM, while treating data of observed traffic patterns, transaction frequencies, or other metrics relevant to security monitoring. The following algorithm 2 utilizes an HMM framework to optimize the selection of vertices and edges for SVED in grid graphs.

Algorithm 2: SVED of $M_{a,b}$ Algorithm

Input: A grid graph $G = M_{a,b}$where a is the number of rows and b is the number of columns.

Output: A SVED set S_{ev}

Initialization:

a. Define the grid graph $M_{a,b}$ with dimensions a and b.

b. Set $S_{ev} = \emptyset$

c. Create an HMM model H with states representing the vertices and edges of the grid.

d. Initialize transition and observation probabilities based on the grid structure.

Model Training

a. Train the HMM using historical data.

b. Determine the transition probabilities $P(s_i \rightarrow s_j)$ between vertices.

c. Establish emission probabilities $P(e_k \mid s_i)$ for observing specific threats from each vertex.

Select Secure Vertices:

For each vertex v_i in $M_{a,b}$

a. Calculate the expected coverage of adjacent edges based on the HMM predictions.

b. If a vertex covers more than one edge, mark it as a candidate for S_{ev}.

Construct the Dominating Set

If ab is even

secure vertices in a grid such that S_{ev} contains $ab/2$ vertices.

If ab is odd

secure vertices in a grid such that S_{ev} contains $\frac{ab+1}{2}$ vertices

---

Validate Coverage:

For each edge e_i in $M_{a,b}$

a. Check if e_i is either incident to a vertex in S_{ev} or adjacent to an edge incident to a vertex in S_{ev}.

b. If any edge is uncovered, adjust S_{ev} by adding additional vertices based on HMM predictions.

Return

Return the set S_{ev} as the result of the algorithm.

The algorithm concludes with an SVED set, S_{ev} that maximizes coverage while minimizing vulnerabilities in the grid graph $M_{a,b}$. This approach ensures continuous monitoring and enhances the security architecture of banking networks.

IV. Application

The proposed SVED algorithm offers the following applications practically to the banking sector. By utilizing the structural properties of these graphs, the algorithm effectively identifies a set of transaction nodes that ensures comprehensive monitoring and redundancy. This is crucial for safeguarding sensitive financial transactions against cyber threats, such as fraud and data breaches. The integration of HMMs enables dynamic adaptation to evolving transaction patterns and threat landscapes, allowing for real-time adjustments in security measures. Furthermore, the algorithm facilitates efficient resource allocation, ensuring that critical network components are consistently monitored without excessive overhead. By employing SVED, financial institutions can bolster their defense mechanisms, thus maintaining the integrity and confidentiality of transactions. Additionally, the methodology is extended to various banking applications, including fraud detection, risk assessment, and compliance monitoring, making it an adaptable tool in the dominion of cybersecurity. Overall, this approach is a positive way of addressing flaws in banking networks, thus promoting trust and security in financial operations.

V. Conclusion

This paper, introduced the concept of SVED in hypercube and grid graphs, which identify minimal SVED sets. As cyber-attacks are posing threats to financial transactions, this framework ensures the optimum choice of vertices and edges such that it can strongly monitor and validate transaction nodes. Also, the focus is on the unique properties of hypercube and grid graphs, both of which are highly relevant for complex, multidimensional banking systems and real-time transaction processing. The integration of HMM further strengthens the framework by allowing for adaptive monitoring based on real-time transaction data Also explore the implications of this work findings on real-world applications, particularly in securing communication infrastructures. This work puts the foundation for future research in graph theory and cybersecurity, providing a robust practice for the defense of transactions in banking systems.

Conflict of Interest:

There is no relevant conflict of interest regarding this paper.

Reference

I. 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, pp. 10, 2020. 10.3390/inventions5010010

II. A. Sahin, and B. Sahin, 'Total edge–vertex domination,' *RAIRO-Theoretical Informatics and Applications*, vol. 54, pp. 1, 2020.

III. A.I. Al-Alawi, and , M.S.A. Al-Bassam, 'The significance of cybersecurity system in helping managing risk in banking and financial sector,' Journal of Xidian University, vol. 14, no. 7, pp. 1523-1536, 2020. 10.37896/jxu14.7/174

IV. A.Q. Stanikzai, and M.A. Shah, 'Evaluation of cyber security threats in banking systems,' In *2021 IEEE Symposium Series on Computational Intelligence (SSCI), IEEE,* pp. 1-4, 2021, December. 10.1109/SSCI50451.2021.9659862

V. B. Dumitrescu, A. Băltoiu, and Ş. Budulan, 'Anomaly detection in graphs of bank transactions for anti money laundering applications,' *IEEE Access*, vol. 10, pp. 47699-47714, 2022. 10.1109/ACCESS.2022.3170467

VI. C. Wang, and H. Zhu, 'Wrongdoing monitor: A graph-based behavioral anomaly detection in cyber security,' *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2703-2718, 2022. 10.1109/TIFS.2022.3191493

VII. D. Angel, A. Arputhamary, and S. Saffren, 'Defense Mechanism for the Nodes of 2-D Meshes and n-cubes,' In *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), IEEE*, pp. 1-4, 2021, February. 10.1109/ICAECT49130.2021.9392622

VIII. D. Angel, G. Uma, and E. Priyadharshini, 'Application of Graph theory to Defend Hypercubes and Matching Graph of Hypercube Structures Against Cyber Threats,' In *2023 First International Conference on Advances in Electrical, Electronics and Computational Intelligence (ICAEECI), IEEE,* pp. 1-4, 2023, October. 10.1109/ICAEECI58247.2023.10370916

IX. H.M. Alzoubi, T.M. Ghazal, M.K. Hasan, A. Alketbi, R. Kamran, N.A. Al-Dmour, and S. Islam, 'Cyber security threats on digital banking,' In *2022 1st International Conference on AI in Cybersecurity (ICAIC), IEEE,* pp. 1-4, 2022, May. 10.1109/ICAIC53980.2022.9896966

X. J. Wang, S. Zhang, Y. Xiao, and R. Song, 'A review on graph neural network methods in financial applications,' *arXiv preprint arXiv:2111.15367*, 2021'

XI. J. Zhang, W. Wang, and E. Zio, 'Study on the Application of Graph Theory Algorithms and Attack Graphs in Cybersecurity Assessment,' In *2023 7th International Conference on System Reliability and Safety (ICSRS), IEEE*, pp. 558-564, 2023, November. 10.1109/ICSRS59833.2023.10381005

XII. K. Golubev, 'Graphical designs and extremal combinatorics,' *Linear Algebra and its Applications*, vol. 604, pp. 490-506, 2020. 10.1016/j.laa.2020.07.012

XIII. K. Zhang, and J. Liu, 'Review on the application of knowledge graph in cyber security assessment," *In IOP Conference Series: Materials Science and Engineering, IOP Publishing*, vol. 768, no. 5, pp. 052103, 2020, March.

XIV. Kulli, V.R., 'Secure edge domination in graphs,' *Annals of Pure and Applied Mathematics*, vol. 12, no. 1, pp. 95-99, 2016.

XV. R. Boutrig, M. Chellali, T.W. Haynes, and S.T. Hedetniemi, 'Vertex-edge domination in graphs,' *Aequationes mathematicae*, vol. 90, pp. 355-366, 2016. 10.1007/s00010-018-0609-9

XVI. R. Jain, and R. Tewari, 'Grid Graph Reachability,' *arXiv preprint arXiv:1902.00488*, 2019.

XVII. T.T. Chelvam, and , M. Sivagami, 'Structure and substructure connectivity of circulant graphs and hypercubes,' *Arab J. Math. Sci*, vol. 27, no. 1, pp. 94-103.

XVIII. Z. DeVivo, and R.K. Hladky, 'New Upper Bounds on the Minimal Domination Numbers of High-Dimensional Hypercubes,' *arXiv preprint arXiv:2409.14621*, 2024. 10.48550/arXiv.2409.14621