Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-A, pp. 3739–3749
DOI : 10.47974/JDMSC-3005

Graph-partition-based attack mitigation in dense mesh networks

Sangeeta Vhatkar [#]
Department of Information Technology
Thakur College of Engineering & Technology
Mumbai 400101
Maharashtra
India

Rupali Mane [†]
Sukruti Kaulgud [§]
Department of Electronics & Telecommunication Engineering
Thakur College of Engineering & Technology
Mumbai 400101
Maharashtra
India

Asmita Bhupesh Marathe [‡]
Department of Computer Science and Engineering (Cyber Security)
Thakur College of Engineering & Technology
Mumbai 400101
Maharashtra
India

Anand Arvind Maha [@]
Department of Artificial Intelligence & Machine Learning
Thakur College of Engineering & Technology
Mumbai 400101
Maharashtra
India

[#] *E-mail:* vhatkarsangeeta@gmail.com
[†] *E-mail:* rupali.mane@thakureducation.org
[§] *E-mail:* sukruti.kaulgud@thakureducation.org
[‡] *E-mail:* asmitamarathe@tcetmumbai.in
[@] *E-mail:* anandmaha007@gmail.com

© Taru Publications

Zahir Aalam *
Department of Computer Science and Engineering (Cyber Security)
Thakur College of Engineering & Technology
Mumbai 400101
Maharashtra
India

Abstract

The attack mitigation technique, presented as graph-partition scheme, enhances the resistance of dense mesh communication network to the fast spreading cyber-attacks. The research work presents an adaptive graph-partitioning framework that incorporates Louvain's community detection, METIS's multi-level partitioning and multi-objective optimization for optimal attack containment. The framework is designed to achieve minimal reverse propagation while maximizing latency, connectivity, load balancing and routing stability in dynamic environments. The Pareto configurations of partitions are obtained by using NSGA-II and Particle Swarm Optimization. Dynamic adaptive partitioning also allows for the protection against wormhole, Sybil and DDoS attacks. Experimental results show that a real-time distributed mesh infrastructure becomes more scalable, resilient and secure with low communication overheads.

Subject Classification: *46N10, 94A60.*

Keywords: *Graph partitioning, Attack mitigation, Dense mesh networks, Multi-objective optimization, NSGA-II, PSO.*

I. Introduction

Graph-Partition-Based Attack Mitigation in Dense Mesh Networks has become an essential research focus to achieve the safety of the highly interconnected and dynamic communication networks. The features of dense mesh networks include redundant edges, decentralized routing and high node density, which are effective in ensuring reliability, but also susceptible to adversarial attacks like wormhole, Sybil attacks and distributed denial-of-service attacks [1, 2]. Conventional defense strategies based on centralized monitoring, or fixed routing policies fail to scale or keep up with the quickly changing threats. Graph-theoretic methods have thus come into the limelight because they are capable of capturing the topology and interactions of a network [3, 4]. In this regard, graph partitioning offers a potential way of partitioning networks into smaller and loosely-coupled subgraphs to constrain the spread of attacks and to allow localized mitigation [5, 6, 7].

Partition-based techniques help to enhance resilience without severely impacting performance by isolating compromised regions and maintaining important connectivity. Figure 1 illustrates partitions of the network as

* *E-mail:* **zahir_aalam@hotmail.com (Corresponding Author)**

framework to isolate attacks and increase resilience. The latest development of community detection, multi-level partitioning and adaptive reconfiguration makes such techniques even more practical to the dynamic environment [8, 9]. In addition, incorporation of optimization frameworks enables trade-off between security goals and the latency, the load, and the throughput limits. The present paper explores the graph-partition-based reduction methods, developing an optimization-based framework, and assessing its performance in adversarial conditions [10, 11]. The proposed solution is to attain scalable, adaptive and robust defenses with efficient network operation over large scale dense mesh deployments [12].

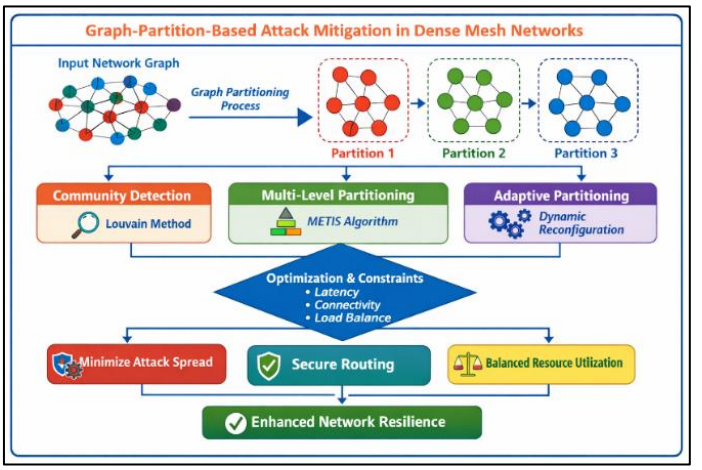


Figure 1

Graph-Partition-Based Attack Mitigation Framework for Dense Mesh Networks

II. Optimization problem formulation with constraints

Develop attack mitigation the objective is to minimize the spread across partitions under the constraints of latency, connectivity, and load balance, provide secure routing, use of available resources effectively and stability of the network when adversaries are present [13].

Network Topology Representation as a graph.

$$G = (V, E) \tag{1}$$

The network is represented using graph notation which characterizes the network as nodes and edges (Eq. 1). It gives the basic abstraction of modeling the communication paths and analyzing the connectivity of dense mesh environments.

$$A = [a_{ij}] \in \mathbb{R}^{N \times N} \tag{2}$$

The adjacency matrix is a weighted representation of the connection between the nodes with each being a measure of the strength of the interaction between the two nodes (Eq. 2). This grid helps in mathematical processes of optimization, partitioning and structural analysis.

$$a_{ij} = \int^{0\,\mathrm{T}} w_{ij(t)} \cdot \delta_{ij(t)dt} \tag{3}$$

The edge weight formulation combines the time-varying behavior of links in the form of weighted interactive and activity pointers (Eq. 3). It is able to capture time dynamics, which allows one to obtain true modeling of changing conditions of communication.

Attack Propagation Modeling

$$S(t) = \sum_{\{i \in V\}} \int^{0\,\mathrm{T}} \left(\sum_{\{j \in N(i)\}} \beta_{ij(t)} \cdot x_{i(t)} \cdot x_{j(t)} \right) dt \tag{4}$$

Attack propagation modeling measures the spreading of the threats among adjacent nodes with time (Eq. 4). It uses the intensity of the interaction, and the state of the node to assess the cascading effects and vulnerability.

Objective Function (Minimization of Attack Spread)

$$\min_P J = \int^{0\,\mathrm{T}} \sum_{\{i,j \in V\}} a_{ij(t)} \cdot x_{i(t)} \cdot x_{j(t)} \cdot \left(1 - \sum_{\{k=1\}_i^{\{K\}p}} k \cdot p_{jk} \right) dt \tag{5}$$

The objective aims at minimizing the spread of attacks through the penalties of inter-partition interactions of affected nodes (Eq. 5). It also provides good isolation and the necessary connectivity and network performances.

Connectivity and Load Balance Constraints

$$\int^{0\,\mathrm{T}} \left| \sum_{\{i\}} p_{ik} \cdot d_{i(t)} - \left(\frac{1}{K} \right) \sum_{\{i\}} d_{i(t)} \right|^2 dt \leq \Omega \tag{6}$$

The load balance constraint provides a fair distribution of traffic among partitions (Eq. 6). It prevents congestion as it curbs deviation of average demand, and makes the utilization of resources to be stable and efficient.

III. Graph Partitioning Methodology

Graph partitioning splits mesh networks that are dense into subgraphs to reduce the extent of attacks, improve containment and connectivity, exploiting structural characteristics and scalable adaptive strategies of network security.

A. *Community Detection*

Community detection uses a modularity optimization to identify node groups in a graph which are densely connected [14]. The Louvain technique can be used effectively to maximize modularity, which can be used to cluster quickly and isolate better the compromised regions in large-scale mesh networks.

Definition of graphs and weights.

$$G = (V, E), W = [w_{ij}] \tag{7}$$

$$k_i = \sum_{\{j \in V\}} w_{ij}, m = \left(\frac{1}{2}\right) \sum_{\{i,j \in V\}} w_{ij} \tag{8}$$

The graph and definition of weight model the network as a network of nodes and weighted edges in which the weight matrix contains the strengths of interaction (Eq. 7). The degree of a node and the total weight of the node are measures of connectivity, with degree being a cumulative measure of node interactions and m a cumulative measure of network weight (Eq. 8). These measures are vital to modularity computing.

Modularity Integral Form Function

$$Q = \left(\frac{1}{2m}\right) \int^0 {}^{\mathrm{T}} \sum_{\{i,j \in V\}} \left[w_{ij(t)} - \frac{k_{i(t)} \cdot k_{j(t)}}{2m(t)} \right] \delta(c_i, c_j) dt \tag{9}$$

The modularity function gauges the quality of community by comparing the real connections with the random connections with time (Eq. 9). Integral form is able to capture the changes in time, and it is more accurate in detecting dynamic communities.

Local Gain in Modularity

$$\Delta Q = \left(\frac{1}{2m}\right) \sum_{\{j \in C\}} \left[w_{ij} - \frac{k_i \cdot k_j}{2m} \right] - \sqrt{\frac{k_i}{2m}} \tag{10}$$

It is the modularity gain that increases with the assigning a node to a community (Eq. 10). It trades off between internal connectivity and anticipated links to give the best clustering choices and discourages weak connections.

B. *Multi-Level Partitioning Techniques (METIS-Based Approaches)*

METIS-based partitioning uses coarsening, partitioning and refining in order to generate balanced graph partitions. It reduces edge cuts and is computationally efficient, and allows parting down of dense and large mesh networks with scalable partitioning. METIS coarsening, partitioning, refinement which makes sure that partitions are balanced, which is described in Figure 2.

Graph Coarsening Phase

$$G^0 \rightarrow G^1 \rightarrow \ldots \rightarrow G_l, w'_{ij} = \int^0 {}^{\mathrm{T}} \varphi(w_{ij(t)}) dt \tag{11}$$

The coarsening step of the graph step-by-step shrink the graph by combining nodes and summing edge weights (Eq. 11). The intrinsic transformation is able to capture time variation, which allows partitioning large scale efficiently with less complexity.

Coarse Graph Partitioning Objective

$$\min \int^0 {}^{\mathrm{T}} \sum_{\{(i,j) \in E_l\}} w_{ij(t)} \cdot (1 - x_i x_j) dt \tag{12}$$

The coarse partitioning objective reduces edge cuts in the reduced graph (Eq. 12) that are weighted. It isolates dissimilar nodes, and maintains

strong internal connectivity, enhancing partition quality and computational performance.

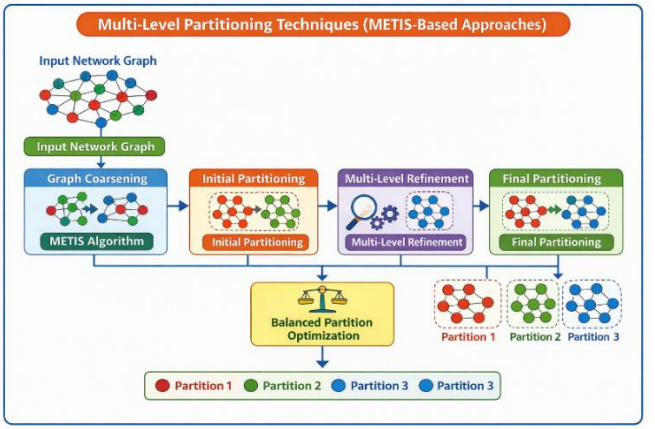


Figure 2

Multi-Level Graph Partitioning Framework Using METIS-Based Coarsening and Refinement Techniques

Balance Constraint with Root Term

$$\sqrt{\sum_{\{i \in V_k\}} d_i^2} \leq B_k, \forall \, partitions \, k \tag{13}$$

Balance constraint is used to balance the weights of the nodes in partitions (Eq. 13). In the root-based formulation, the variance of partition size is kept, avoiding overload and ensuring a balance in computational and communication.

Uncoarsening and Refinement

$$\min \int^{0}{}^{\mathrm{T}} \left[Cut(G,t) + \lambda \sum_{\{k\}}^{2} \left(Load_{k(t)} - \bar{Load}(t) \right) \right] dt \tag{14}$$

The uncoarsening and refinement stage recovers the original graph, and optimizes the quality of partitions (Eq. 14). It reduces the size of the cuts and imbalance of the loads that will result in a better final partitioning accuracy and stability.

Final Partition Optimization

$$\min_X \int^{0}{}^{\mathrm{T}} \sum_{\{(i,j) \in E\}} w_{ij(t)} \cdot \left| x_i - x_j \right|^2 dt \tag{15}$$

The last partition optimization reduces the differences between edges of the nodes which belong to different partitions (Eq. 15). It improves cohesion in clustering, minimizes the cost of communication and also increases the effectiveness of the entire network segmentation.

C. *Threat Model and Attack Scenarios*

The high level of decentralization in routing, multi-hop communication and dynamic topology adaptation of dense mesh networks makes them highly vulnerable to coordinated cyberattacks. The proposed mitigation scheme based on graph-partition relies on multiple adversarial attack scenarios which can have an impact on the stability of routing, integrity of the nodes, and propagation of malicious messages in the interconnected partitions. The threat model entails that adversaries can be a compromised node inside the network or a malicious attacker trying to compromise communication channels, overload network resources or affect the packet forwarding.

1. Wormhole Attack Model

The wormhole attack mode involves two adversarial nodes forming a low latency connection between two far away areas of the network to create a misleading connection in the routing. Legitimate nodes mistakenly believe that the wormhole communication path is the shortest path for communication, and thus send huge amounts of traffic through compromised routes. This behavior allows traffic to be selectively forwarded, packet manipulation, and packet interception. The proposed partitioning framework can help to reduce wormhole propagation by isolating suspicious inter-partition communication edges and minimizing abnormal shortcut connectivity by adaptively optimizing graphs according to the communication pattern.

2. Sybil Attack Propagation

Sybil attacks are simulated using the network topology by creating several fake identities by the adversarial nodes. These forged identities are used to influence routing decisions, to enhance voting influence and to interfere with communication protocols based on trust. Sybil nodes in meshes with high density can very quickly gain more influence by establishing redundant links with other partitions. The proposed framework aims at reducing the propagation of Sybils by identifying the illegal clusters of nodes based on the concept of modularity based community analysis and by detecting the identity inconsistencies in the partitions through dynamic partition reconfiguration.

3. Distributed Denial-of-Service (DDoS) attacks.

The DDoS attack model is based on multiple overflowing of network bandwidth, computational resources and buffer capacities by many compromised nodes flooding the network with excessive routing requests and packet flooding traffic. These kinds of attacks result in higher routing delays, lower packet delivery ratio and cause paths of communication within dense mesh infrastructures to become unstable. The proposed

graph-partitioning mechanism involves partitioning the graph into subgraphs based on the maximum set of nodes affected by the flooding and redistributing the traffic loads among them using optimized partition balancing strategies, which helps to limit the spreading of the flooding.

IV. Objective Function for Minimizing Attack Spread

The objective aims to reduce the spread of attacks through minimizing inter-partition connectivity of compromised nodes, cut edge optimisation and isolating the affected areas without affecting necessary communication paths and network performance.

$$G = (V, E), x_{i(t)} \in \{0,1\}, w_{ij(t)} \tag{16}$$

$$k_{i(t)} = \sum_{\{j\}} w_{ij(t)} \tag{17}$$

The network is modeled by the graph and state, which consists of nodes, edges and attack states as a function of time (Eq. 16). binary state variables represent compromised nodes, and it is possible to dynamically track the adversarial influence. The degree of nodes over time is the cumulative strength of interaction of each node (Eq. 17). It shows the degree of connectivity, which affects the degree of vulnerability and spreading ability in the network structure.

$$E(t) = \sum_{\{i,j \in V\}} w_{ij(t)} \cdot x_{i(t)} \cdot x_{j(t)} \tag{18}$$

A propagation energy of attacks is a measure of the immediate propagation of threats between connected nodes (Eq. 18). It takes a combination of edge weights and node states to quantify the risk levels due to interactions.

$$S_{norm} = \sqrt{\int^{0\,\mathrm{T}} \left(\sum_{\{i,j\}} w_{ij(t)} \cdot x_{i(t)} \cdot x_{j(t)} \right)^2 dt} \tag{19}$$

The normalized spread brings about root-based scaling to level huge variations (Eq. 19). It makes sure that the propagation intensity is evaluated in a balanced manner such that extreme values are not predominant in optimization.

V. Result and Discussion

Findings show that graph-partition based mitigation is much more effective in preventing the spread of the attack and detecting it than traditional ones. The isolation created by partitioning helps to reduce cascading failures, by isolating compromised nodes. Latency is kept at acceptable levels and throughput and load distribution is also enhanced.

Table 1

Performance Evaluation of Graph-Partition-Based Attack Mitigation

Metric	Conventional Routing	Static Partitioning	Graph-Partition-Based
Packet Delivery Ratio (%)	87.6	91.8	96.3
Attack Detection Rate (%)	63.4	75.9	90.7
Attack Spread Reduction (%)	42.5	61.3	84.9
Routing Latency (ms)	192	168	141

The performance of graph-partition based attack mitigation is compared to that of conventional routing and a fixed partitioning as seen in Table 1. Figure 3 presents heatmap that visualizes the routing performance at different strategies in partitions.

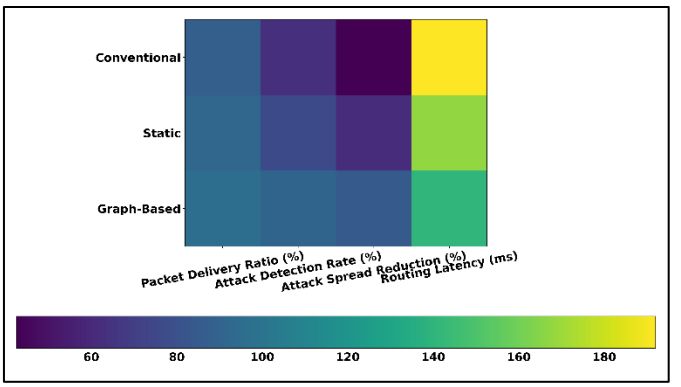


Figure 3

Graph-Partition-Based Routing Performance Heatmap

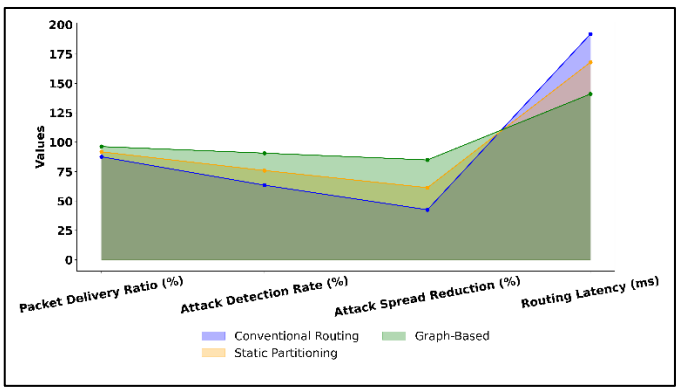


Figure 4

Attack Mitigation and Routing Efficiency Trends

The proposed algorithm has the best packet delivery ratio of 96.3 meaning that it has better reliability in adversarial conditions. Figure 4 indicates trends of the mitigation of attacks and routing efficiency. The probability of attack detection is also greatly improved to 90.7, which is indicative of improved threat detection.

It is interesting to note that the reduction in attack spread is 84.9, which shows that it is possible to contain the attacks using partition isolation.

VI. Conclusion

This paper demonstrated an attack mitigation scheme of dense mesh networks that is based on graph-partition and combines community detection, multi-level partitioning, and adaptive reconfiguration. Using the constrained multi-objective optimization task to formulate the problem is effective to balance security, latency, connectivity, and distribution of load. Applications of NSGA-II and PSO can effectively search the Pareto-optimal solutions, and it can be strongly applied in various adversarial conditions. Findings validate that isolation using partitions is very useful in curbing the spread of the attack without affecting the network functionality and quality of service. The framework facilitates any changes in topology and topography as well as changes in threats thus it is adaptable to be used in large scale distributed environment in real time.

References

[1] M. Oehlers and B. Fabian, "Graph metrics for network robustness—A survey," *Mathematics*, vol. 9, no. 8, Art. no. 895 (2021), doi: 10.3390/math9080895.

[2] K. Koo, D. Moon, J.-H. Huh, S.-H. Jung, and H. Lee, "Attack graph generation with machine learning for network security," *Electronics*, vol. 11, no. 9, Art. no. 1332 (2022), doi: 10.3390/electronics11091332.

[3] F. Miao, X. Zhou, S. Xiao, and S. Zhang, "A graph similarity algorithm based on graph partitioning and attention mechanism," *Electronics*, vol. 13, no. 19, Art. no. 3794 (2024), doi: 10.3390/electronics13193794.

[4] Y. Listiana, L. Susilowati, S. Slamin, and K. Dliou, "The central local metric dimension of graphs with a single central vertex," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 28, no. 6, pp. 2297–2308 (2025), doi: 10.47974/JDMSC-2228.

[5] P. Khobragade, B. Thakran, P. K. Dhankar, P. Dasarwar, C. Vaidya, and K. Dhote, "Improving intrusion detection systems using machine learning algorithms for real-time network security monitoring," in *Proc. 1st Int. Conf. Data Science and Intelligent Network Com-*

puting (ICDSINC), Raipur, India, pp. 160–165 (2025), doi: 10.1109/ICDSINC66221.2025.11448255.

[6] S. Karageorgiou and V. Karyotis, "Markov-based malware propagation modeling and analysis in multi-layer networks," *Network*, vol. 2, no. 3, pp. 456–478 (2022), doi: 10.3390/network2030028.

[7] V. Yadav, A. P. Kharade, A. Rawat, D. S. Asudani, and K. Anitha, "Strategic investment approaches for building robust computer security frameworks within organizational networks," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1661–1669 (2026), doi: 10.47974/JIOS-2256.

[8] S. Charkhabi, P. Samimi, S. S. Bagui, D. Mink, and S. C. Bagui, "Node classification of network threats leveraging graph-based characterizations using Memgraph," *Computers*, vol. 13, no. 7, Art. no. 171 (2024), doi: 10.3390/computers13070171.

[9] A Cilfone, L. Davoli, L. Belli, and G. Ferrari, "Wireless mesh networking: An IoT-oriented perspective survey on relevant technologies," *Future Internet*, vol. 11, no. 4, Art. no. 99 (2019), doi: 10.3390/fi11040099.

[10] M. Kalinin, E. Zavadskii, and A. Busygin, "A graph-based technique for securing the distributed cyber-physical system infrastructure," *Sensors*, vol. 23, no. 21, Art. no. 8724 (2023), doi: 10.3390/s23218724.

[11] R. C. Poonia, T. Singh, C. K. Rajashri, D. Mondal, and S. M. Patil, "Optimizing communication system security through comprehensive testing and intelligent network configurations," *Journal of Information and Optimization Sciences*, vol. 47, no. 5-A, pp. 1709–1717 (2026), doi: 10.47974/JIOS-2261.

[12] X. Zhang, B. Hu, S. Liu, Q. Sun, and L. Chen, "AttenFlow: Context-aware architecture with consensus-based retrieval and graph attention for automated document processing," *Applied Sciences*, vol. 15, no. 13, Art. no. 7517 (2025), doi: 10.3390/app15137517.

[13] D. Kanellopoulos, V. K. Sharma, T. Panagiotakopoulos, and A. Kameas, "Networking architectures and protocols for IoT applications in smart cities: Recent developments and perspectives," *Electronics*, vol. 12, no. 11, Art. no. 2490 (2023), doi: 10.3390/electronics12112490.

[14] M. François, P.-E. Arduin, and M. Merad, "Physics-informed graph neural networks for attack path prediction," *Journal of Cybersecurity and Privacy*, vol. 5, no. 2, Art. no. 15 (2025), doi: 10.3390/jcp5020015.

Received April, 2026