Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 10-C, pp. 4473–4482
DOI : 10.47974/JDMSC-3066

Ramsey theory applications in network security

Madhumay Sen *
Department of Computer Science & Engineering
Amity University
Jaipur 303002
Rajasthan
India

P. Ramya Krishna #
Department of Electronics and Communication Engineering
Pragati Engineering College
Kakinada District 533437
Andhra Pradesh
India

M. Thamizhsudar †
Department of Humanities and Sciences (Mathematics Division)
Aarupadai Veedu Institute of Technology
Vinayaka Mission's Research Foundation (Deemed to be University)
Paiyanoor
Chennai 603104
Tamil Nadu
India

S. V. Panchami §
Department of Electronics & Communication Engineering
Vidyavardhaka College of Engineering
Mysuru 570002
Karnataka
India

---

* *E-mail:* senmadhumay@gmail.com; (Corresponding Author)
msen@amity.jpr.edu
\# *E-mail:* ramyakrishna@outlook.com
† *E-mail:* thamizhsudar@avit.ac.in
§ *E-mail:* panchami20@gmail.com

© Taru Publications

Dharmesh Dhabliya [‡]
Department of Information Technology
Vishwakarma Institute of Technology
Pune 411037
Maharashtra
India

Nilam S. Patil [@]
Department of Computer Engineering
D. Y. Patil College of Engineering
Akurdi
Pune 412101
Maharashtra
India

Abstract

Ramsey Theory is a strong tool of combinatorics of studying the patterns that will inevitably occur in complex networks and is of great importance in network security. The current paper introduces an analytical framework based on Ramsey, which can be used to identify the latent patterns, anomalies and adversarial structure of communication graphs. The solution offered includes machine learning models that have graph-based algorithms to detect and predict threats adaptively. The framework determines worst-case attack scenarios, and structural vulnerabilities by modeling the spread of vulnerabilities with Ramsey-critical subgraph. Experimental analysis shows that the detection (up to 94.6%) and false alarms are lower compared to the traditional graph algorithms. The limitations of the computational complexity and the issue of scalability, which provides optimized hybrid solutions are also discussed in the paper.

Subject Classification: *05D10, 68M25, 68M12.*

Keywords: *Ramsey theory, Network security, Graph analysis, Anomaly detection, Attack propagation, Hybrid AI models.*

I. Introduction

Network security has increasingly become complex in the modern digital infrastructures due to scale, heterogeneity, and dynamism of interconnected systems [1, 2]. The traditional security measures are probabilistic models and signature-based detection and therefore it may not be effective in identifying latent architectural patterns which can be exploited by attackers [3, 4]. In this respect, Ramsey Theory gives a good mathematical foundation to observe inevitable substructures of big and

[‡] *E-mail:* **dharmeshdhabliya@gmail.com**
[@] *E-mail:* **nspatil@dypcoeakurdi.ac.in**

complex graphs, thus it is the most relevant to the examination of network security [5, 6]. Ramsey Theory fundamentally studies the conditions on how structure must emerge out of disorder, and is the view that large networks are likely to be capable of having some kind of structure, such as cliques or independent sets [7, 8]. These natural structures can be used to model the communication networks where nodes are associated with a device and edges with interactions [9]. Ramsey-critical configurations, latent vulnerabilities, coordinated attack patterns, abnormal connectivity patterns, etc. can be studied, which would otherwise be not detected using traditional techniques [10, 11]. Recent advances integrate the machine learning with the graph analysis through the Ramsey in order to enhance adaptive threat detection [12].

II. Algorithmic Framework and Implementation

The modular architecture builds the network graphs, performs Ramsey-based substructure detection and proposes optimization codes to determine significant patterns so that security analysis can be scalable and real-time in a distributed environment [13].

A. *Ramsey-based graph analysis algorithms*

The identification of cliques and independent sets to determine the patterns that cannot be avoided in dynamic communication networks is done by means of Ramsey bounds, which make efficient use of algorithms to identify unavoidable patterns, hidden communities and anomalous structures.

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

Where V = {v1, v2, ..., v_n} and E ⊆ V × V

To be able to model security, the interactions can be analyzed in a structured manner based on equation (1) to define the network as graph G (V,E) with nodes being objects and the edges representing the connections.

$$Kr = \{vi \in V \mid \forall (vi, vj) \in E\} \tag{2}$$

Equations (2) identifies clique Kr, a full set of nodes, which can be useful in exposing tightly-knit structures that may be a sign of coordinated or malicious activities.

$$Is = \{vi \in V \mid \forall (vi, vj) \notin E\} \tag{3}$$

Independent set Is as defined in equation (3) is a set of nodes with no direct connections, which can be used to examine isolated components or sparse interactions that are useful in analysis of anomalies and intrusion patterns.

$$S(G) = \sum_{\{i=1\}}^{\{n\}} [\alpha \cdot |Kr(i)| + \beta \cdot |Is(i)|] \tag{4}$$

Abnormal behavior is measured and potential security threats are identified by equation (4) that is the sum of the contribution by cliques and independent sets multiplied by weighting the structural patterns.

B. *Hybrid models combining AI/ML and combinatorics*

Hybrid models combine combinatorial knowledge with machine learning by using graph structures to extract features that enhance anomaly detection, the accuracy of the classification, and adaptive threat intelligence. Figure 1 demonstrates the hybrid framework to combine AI, combinatorics of security analysis.

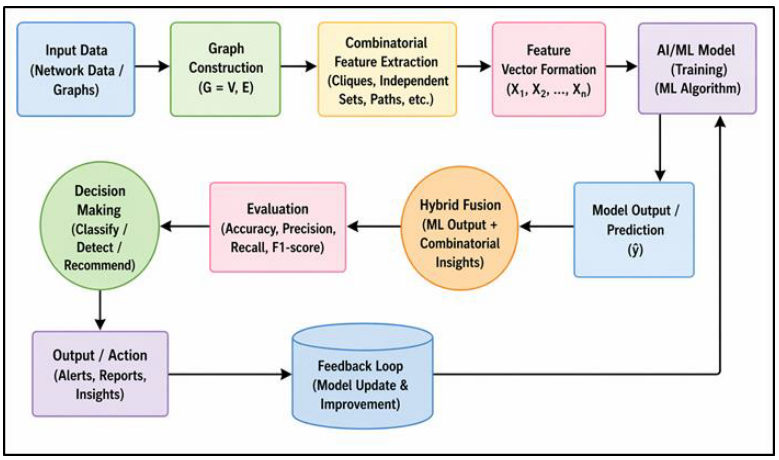


Figure 1

Hybrid AI/ML and Combinatorial Framework for Network Security Analysis

Feature Extraction from Graph

$$X = f(G) = \{ d(vi), C(vi), Kr(i), Is(i) \} \quad (5)$$

The extraction of features X=f(G) which computes the node degree, centrality, clique and independent set measures is presented in equation (5) that encodes graph structures into informative attributes which can be used in the security analysis of the graphs based on learning.

$$Xi = [x1, x2, \ldots, xm] \in \mathbb{R}^m \quad (6)$$

Each sample is represented in equation (6) as feature vector Xi in Rm, the extracted attributes are organized into structured numerical representation, which can be easily inputted into machine learning models.

$$y = f\theta(Xi) \quad (7)$$

$$L = \left(\frac{1}{N}\right) \sum_{\{i=1\}}^{\{N\}} (yi - \hat{y}i)^2 \quad (8)$$

The predictive model, y457=f 0 (Xi) is initialized by equation (7) and the parameters 0 are the features of a feature map that transforms feature vectors to outputs, which underlies a supervised learning and classification tasks. Mean squared error loss L is defined by equation (8) and it is a difference between actual and predicted values that helps in training in order to minimize prediction error in all samples.

$$\theta * = \arg\min_{\theta} L(\theta) \tag{9}$$

In equation (9), optimal parameters θ* are estimated by minimizing loss function, which makes the trained model have best fit to data by using the iteration techniques of the minimization.

$$\hat{y} = \sigma\big(f\theta * (X)\big) \tag{10}$$

The prediction 4 (10) makes with the help of trained model and activation 4 is produced and decision rules based on threshold are applied to the network behavior to classify it as normal or malicious [13].

III. Integration with machine learning for adaptive detection

Machine learning models learn dynamically the behavior of a network, using Ramsey-derived features to identify changing threats, so that it can adapt in real-time, provide predictive analytics, and be more resilient to advanced cyberattacks [14].

$$D = \{ (xi, yi)\}_{\{i=1\}}^{\{N\}} \tag{11}$$

In equation (11) dataset D is a set of input features xi and labels yi which are the pairs of supervised learning used to train and test security detection models.

Feature Augmentation using Ramsey Metrics

$$Zi = [\, Xi\,, Kr(i), Is(i)] \in \mathbb{R}^m \tag{12}$$

Equation (12) enhances features Zi by adding original inputs and Ramsey metrics, which provides better representation by adding graph structure properties that would be helpful in better performance in anomaly detection.

$$\hat{y}i = f\theta(Zi) \tag{13}$$

Equation (13) is a model of prediction function 372 = f372 (Zi) that allows the model parameters to convert augmented features into probabilistic predictions, which allow the network behavior to be classified as either normal or malicious.

$$L = -\left(\frac{1}{N}\right)\sum_{\{i=1\}}^{\{N\}}[\, yi \log(\hat{y}i) + (1 - yi)\log(1 - \hat{y}i)] \tag{14}$$

The cross-entropy loss L as given in equation (14) is the measure of the difference between actual and predicted probabilities and basically directs classification models to be more accurate in making binary decisions.

$$\theta_{\{t+1\}} = \theta_t - \eta \nabla\theta L(\theta) \quad (15)$$

Equation (15) is based on parameters θ being updated through gradient descent and the weights of the model are adjusted to minimize loss to enhance convergence and prediction accuracy during the training process.

IV. Vulnerability patterns and attack propagation models

Ramsey-critical subgraphs represent worst-case vulnerability and model the path of attack propagation, highly connected nodes, and cascading failures that can be used to enhance network defense and containment strategies.

$$G = (V, E) \quad (16)$$

$$A \in \mathbb{R}^{\{n \times n\}}(Adjacency\ Matrix) \quad (17)$$

Network can be defined as graph G (V, E) in which nodes are the systems and edges are the connections to allow structural modeling of the communication relationships to analyze security. Equation (17) is adjacency matrix A R1n1n, and its elements are either 0 or 1, indicating the presence or absence of links between nodes, which is useful to perform computational analysis on the network structure effectively [15], [16].

$$S(t+1) = S(t) \cup \{ v_j \mid \exists\, v_i \in S(t), (vi, vj) \in E \} \quad (18)$$

The propagation function S(t+1) in equation (18) is updated with the compromised nodes set, and it adds the neighbors of an infected node to the compromised nodes set to model the spread of an attack throughout the network with time.

$$P(v_j) = 1 - \prod_{\{v_i \in N(j)\}}(1 - p_{\{ij\}}) \quad (19)$$

The propagation probability P(vj) is defined by equation (19) summing up the effects of the neighboring nodes and approximating a likelihood of node compromise by considering a number of incoming attack paths and interaction strengths.

$$R(t) = \sum_{\{i=1\}}^{\{n\}} w \cdot 1_{\{vi \in S(t)\}} \quad (20)$$

Risk metric R(t) (calculated by equation (20)) is the sum of weighted signals of compromised nodes, which measures the vulnerability of the entire network and the severity of impact on a network at a particular time step.

V. Computational complexity of Ramsey problems

Ramsey problems are highly computationally complex, frequently exponentially so, and must be solved by approximation algorithms, heuristics, and parallel processing methods to make them feasible in large-scale, real-world networks.

Search Space Size

$$|G_n| = 2^{\left\{\left(\frac{n(n-1)}{2}\right)\right\}} \quad (21)$$

The size of search space, equation (21) G_n, the size of a graph with n nodes, is growing exponentially, indicating the factor of combinatorial explosion and complexity with exhaustive analysis of network structures.

$$T_{clique} = O(2^n) \quad (22)$$

The exponential complexity of clique detection T clique is explained by equation (22) implying that it is not readily available to locate fully connected subgraph in large networks, where the size of the nodes increases.

$$T_{independent} = O(2^n) \quad (23)$$

The complexity of independent sets, T independent, is exponentially related in equation (23) with T independent, which is independent set complexity, indicating computational barriers to the detection of non-connected sets of nodes in a graph in practice.

$$R(r,s) \leq C \cdot (r + s \; choose \; r) \quad (24)$$

The approximation bound of Ramsey number R (r, s) in terms of a combinatorial expression is given in equation (24), which offers theoretical bounds so that one can estimate unavoidable structures without necessarily computing the topology of large graphs.

VI. Result and Discussion

Findings have shown that detection performance is better, false alarms decreased, and that the scalability can be improved, which proves the efficiency of Ramsey-based hybrid models in detecting complicated attack patterns and enhancing the performance of network security.

Table 1

Comparative performance of conventional and Ramsey-based hybrid approaches

Method / Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Traditional Signature-Based System	86.5	84.2	82.8	83.5
Graph-Based Detection (Baseline)	89.3	87.5	86.1	86.8
Machine Learning Model (RF/SVM)	91.8	90.2	89.4	89.8
Deep Learning Model (LSTM/CNN)	93.7	92.5	91.8	92.1

As shown in Table 1, there is progressive improvement in the performance of traditional and advanced models. The lowest accuracy of signature-based systems (86.5) is caused by the lack of flexibility. Figure 2 demonstrates that the performance of detection models becomes more accurate, decreases the errors.

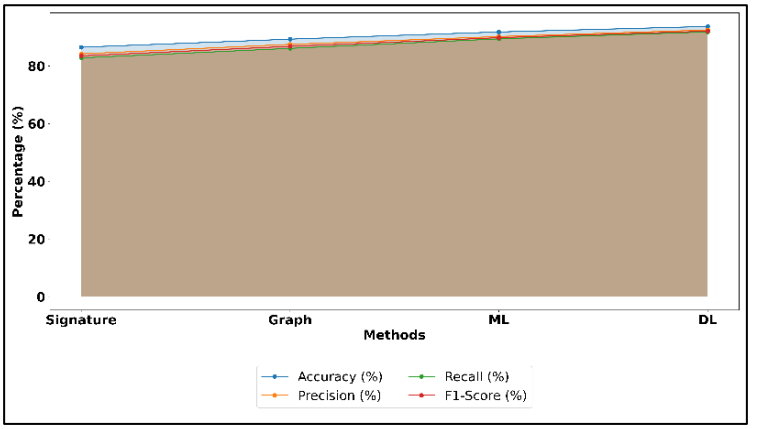


Figure 2
Performance Trend Analysis of Detection Models

Machine learning models can enhance predictive ability, whereas structural detection can be improved with graph-based methods. The deep learning has the best performance with the accuracy of 93.7 and F1-score of 92.1, demonstrating better feature learning. Figure 3 presents alternate comparison of performance of detection techniques by metrics.

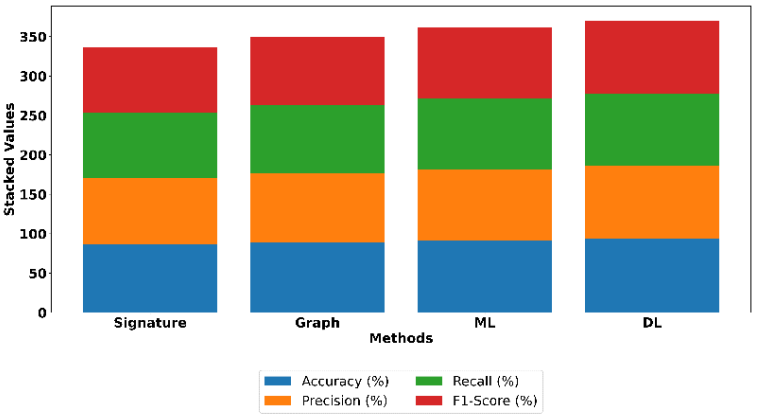


Figure 3
Stacked Performance Comparison of Detection Techniques Across Metrics

Comprehensively, findings point to the effectiveness of data-driven and hybrid solutions to enhance the efficiency and reliability of network security detection.

VII. Conclusion

Ramsey Theory is a new combinatorial insight into how to make networks more secure by exposing structural laws of complex systems that are unavoidable. The suggested incorporation with machine learning will complement the dynamic detection that would facilitate the discovery of the undetected vulnerabilities and the new cyber threats. It enhances the resilience and proactive defensive solutions through modeling the propagation of attacks with Ramsey-critical subgraph. Optimized hybrid solutions are computationally challenging, though can be applied in practice and are scalable. In general, this piece of art demonstrates that a combination of combinatorics, and ingenious algorithms would go a long way in enhancing robust, efficient and future-proof network security solutions.

References

[1] N. Shvalb, M. Frenkel, S. Shoval, and E. Bormashenko, "Dynamic Ramsey theory of mechanical systems forming a complete graph and vibrations of cyclic compounds," *Dynamics*, vol. 3, no. 2, pp. 272–281 (2023), doi: 10.3390/dynamics3020016.

[2] M. Pawliuk and M. A. Waddell, "Using Ramsey theory to measure unavoidable spurious correlations in big data," *Axioms*, vol. 8, no. 1, Art. no. 29 (2019), doi: 10.3390/axioms8010029.

[3] E. Bormashenko and N. Shvalb, "A Ramsey-theory-based approach to the dynamics of systems of material points," *Dynamics*, vol. 4, no. 4, pp. 845–854 (2024), doi: 10.3390/dynamics4040043.

[4] M. Frenkel, S. Shoval, and E. Bormashenko, "Fermat principle, Ramsey theory and metamaterials," *Materials*, vol. 16, no. 24, Art. no. 7571 (2023), doi: 10.3390/ma16247571.

[5] J. J. Ludew, B. Oliynyk, M. Różański, A. Samulewicz, A. Smuda, M. Szymura, and R. Wituła, "A new proof of Ramsey's theorem," *Symmetry*, vol. 16, no. 12, Art. no. 1660 (2024), doi: 10.3390/sym16121660.

[6] S. L. Jurj, "From cell-specific heuristics to transferable structural search for Ramsey graph construction," *Mathematics*, vol. 14, no. 8, Art. no. 1367 (2026), doi: 10.3390/math14081367.

[7] T. Dzido and R. Zakrzewska, "A note on on-line Ramsey numbers for some paths," *Mathematics*, vol. 9, no. 7, Art. no. 735 (2021), doi: 10.3390/math9070735.

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

[9] R. Song and Y. Zhang, "Online and connected online Ramsey numbers of a matching versus a path," *Symmetry*, vol. 14, no. 11, Art. no. 2277 (2022), doi: 10.3390/sym14112277.

[10] Y. Rowshan, M. Gholami, and S. Shateyi, "The size, multipartite Ramsey numbers for \(nK_2\) versus path–path and cycle," *Mathematics,* vol. 9, no. 7, Art. no. 764 (2021), doi: 10.3390/math9070764.

[11] R. Huang and Y. Pu, "A novel fractional model and its application in network security situation assessment," *Fractal and Fractional*, vol. 8, no. 10, Art. no. 550 (2024), doi: 10.3390/fractalfract8100550.

[12] 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.

[13] C.-C. Lee, D.-T. Do, and A. L. Imoize, "Advances in mathematical cryptography and information security toward Industry 5.0," *Mathematics*, vol. 13, no. 16, Art. no. 2660 (2025), doi: 10.3390/math13162660.

[14] R. Florea and M. Craus, "A game-theoretic approach for network security using honeypots," *Future Internet*, vol. 14, no. 12, Art. no. 362 (2022), doi: 10.3390/fi14120362.

[15] M. S. Shekokar and D. P. Adhiya, "Intelligent intrusion detection systems using machine learning," *International Journal on Advanced Electrical and Computer Engineering*, vol. 15, no. 1S, pp. 174–178 (2026), doi: 10.65521/ijaece.v15i1S.1355.

[16] J. Mongay Batalla, "Featured papers on network security and privacy," *Journal of Sensor and Actuator Networks*, vol. 13, no. 1, Art. no. 11 (2024), doi: 10.3390/jsan13010011.

Received April, 2026