Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

LETTER

Resilience of the Invisible Internet Project: A Computational Analysis

Siddique Abubakr Muntaka | **Jacques Bou Abdo**

[1]School of Information Technology, University of Cincinnati, OH, USA

Correspondence
Corresponding author Siddique Abubakr Muntaka.
Email: muntaksr@mail.uc.edu

Present address
2610 University Cir, Cincinnati OH 45221.

Abstract

The Invisible Internet Project (I2P) is a decentralized peer-to-peer anonymity network that protects users' privacy by routing traffic through encrypted tunnels across volunteer-run routers (nodes). Its distributed nature raises critical questions about structural resilience, specifically, how well it can withstand random (stochastic) failures and targeted (adversarial) attacks. This study models I2P's overlay using three representative network graphs or topologies: Random Graph (RG), Scale-Free (SF), and a theoretical modeling of I2P's network, herein referred to as *I2P Prime (I2P')*, all experimented with 50,000 nodes (peers) each to reflect the real-world conditions of the I2P network. Simulations under random node removals show that all three networks retain large connected components (LCC) beyond 50% node loss, with *I2P Prime* maintaining superior efficiency. However, targeted attacks based on degree or betweenness centrality reveal substantial vulnerabilities. The SF network model of I2P collapsed rapidly, often below 30% node removal due to its hub-centric design. In contrast, *I2P Prime* exhibits stronger fault tolerance, requiring nearly 50% of critical nodes to be removed before global connectivity fails. These findings underscore the structural advantages of topologies like *I2P Prime*, which combines distributed connectivity and resilience to percolation and Perturbation. For developers, enhanced adaptive peer selection and dynamic routing mechanisms could enhance robustness without undermining anonymity. For policymakers, our results highlight how targeted interventions might fragment illicit activity with minimal collateral impact. This work provides actionable insights into designing resilient anonymity networks that preserve privacy under stochastic and adversarial attacks.

KEYWORDS
Invisible Internet Project (I2P), Network Resilience, Percolation Theory, Anonymity Networks, Decentralized Networks, privacy, Cybersecurity

1 | INTRODUCTION

The Invisible Internet Project (I2P) has emerged as a leading anonymity network. It offers a fully decentralized platform for secure communication through volunteer-run routers (nodes) that create encrypted tunnels for communication. I2P obscures both the origin and destination of messages[1]. It protects sensitive users such as journalists, political dissidents, and whistleblowers from pervasive surveillance and censorship[2,3]. However, the decentralization that empowers these privacy guarantees raises critical questions about the network's structural resilience, as evident in overlay networks[4]. I2P's network resilience relies on surviving random node failures and targeted attacks on critical routers (nodes). Understanding the network's resilience to such disruptions is critical for addressing evolving challenges in cyberspace. On one hand, robustness to random failures ensures that legitimate users retain reliable connectivity despite everyday outages. On the other hand, vulnerability to targeted (adversarial) attacks could enable malicious actors, or conversely, law enforcement agencies (LEA's), to rapidly fragment this overlay network (I2P), impeding anonymous communication or isolating illicit traffic with precision[5,6]. Prior studies have characterized other overlay networks, but they typically examine fewer nodes or smaller network sizes and fail to represent near-real-world network

Abbreviations: ANA, anti-nuclear antibodies; APC, antigen-presenting cells; IRF, interferon regulatory factor.

sizes accurately [7,4]. Therefore, a comprehensive assessment of I2P's resilience under stochastic and adversarial failures remains underexplored. In this work, we bridge the research gap by presenting the resilience study of the network layer of I2P across three representative network models (topologies) as network graphs: the Random Graph (RG), Scale-Free (SF), and a theoretical modeling of I2P's network (I2P Prime) [1]. Our findings offer deep insights into structural vulnerabilities and identify thresholds critical to the network's integrity, guiding both defensive strategies for developers and targeted interventions for policymakers and cybersecurity stakeholders.

The remainder of this paper is organized as follows. Section 2 reviews related work on anonymity networks and network resilience. Section 3 describes our computational methodology using Mesa agent-based modeling (ABM) simulations. Section 4 presents our findings and interprets their implications. Finally, Section 5 discusses the impact, and Section 6 concludes with limitations and provides guidance for future research.

2 | LITERATURE REVIEW

Network resilience is defined as the ability for a system to maintain functionality despite disruptions [8]. Pioneering works by Albert, Jeong, and Barabási [9,10] demonstrated the "robust yet fragile" nature of scale-free networks, which are characterized by a few highly connected hubs. These networks exhibit resilience to random failures but are vulnerable to targeted attacks on the central nodes. Percolation theory, a foundational concept in understanding network resilience, explores the formation and robustness of large-scale connected structures within complex networks, highlighting how induced effects can trigger abrupt and discontinuous connectivity transitions [11]. Gao, Barzel, and Barabási refined the resilience analysis by demonstrating that network robustness can often be summarized effectively through two averaged parameters, simplifying the evaluation of complex system states [12]. The critical thresholds identified through percolation theory have significantly advanced the understanding of cascading network failures [13], with applications spanning diverse infrastructure systems, including power grids and transportation networks [14].

Tor's resilience has been the subject of extensive research, with studies analyzing its robustness to node failures and various attack vectors [15]. However, I2P's architecture, which utilizes a highly decentralized peer-to-peer structure and garlic routing (combining multiple messages into a single encrypted packet), raises unique concerns about resilience [7]. Figure 1 shows an I2P router fetching peer (node) data from the network database (netDb) and building separate outbound and inbound tunnels [16]. Alice's gateway path and Bob's endpoint path pass through routers (nodes) R1 to R17 (as gateways, participants, or endpoints), complicating resilience analysis regarding percolation for the I2P garlic-routed network.

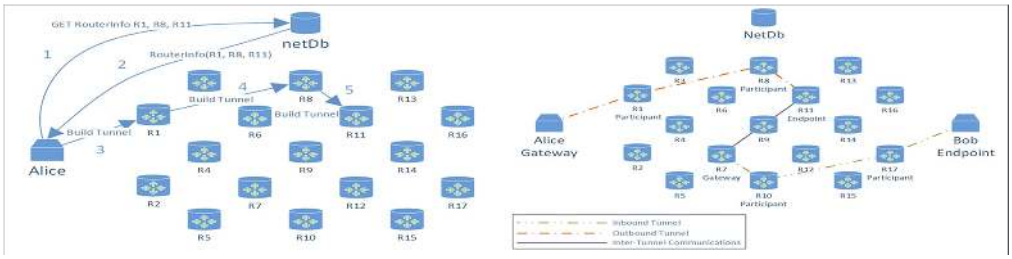

FIGURE 1 Communication in I2P network using inbound and outbound tunnels [16].

Existing research on I2P has identified weaknesses that can be exploited in specific attacks, such as eclipse attacks [6],and network database (netDb) attacks [17]. The existing research does not comprehensively evaluate I2P's resilience to random and targeted failures. Additionally, I2P's network topology constantly evolves, with nodes joining and leaving frequently [18], which complicates resilience assessments and underscores the necessity of large-scale evaluations.

This study addresses these critical gaps by employing computational simulations informed by percolation theory and assessing resilience across three network models of I2P as network graphs: a Random Graph (RG) network, a Scale-Free (SF) network, and I2P' network. According to [19], a random graph is a type of network where connections (edges) between nodes (vertices) are assigned randomly according to some probability. For instance, Erdős–Rényi random graph model $G(n, p)$ constructs a network

of n labeled nodes by simply "flipping a coin" (probability p) for each of the $\binom{n}{2}$ possible edges. In a scale-free network, the degree distribution follows $P(k) \propto k^{-\alpha}$ ($\alpha \approx 2$–3), yielding a few highly connected hubs and many low-degree nodes[20].

3 | METHODOLOGY

To investigate the structural resilience of the I2P network, we developed a large-scale simulation using Mesa (Python framework) for agent-based modeling (ABM) on Google Colab. Three different networks were constructed to model I2P: a Random Graph (RG), a Scale-Free (SF) network, and I2P Prime (I2P'). Each network contained 50,000 nodes, approximating the current scale of the real-world I2P network[21]. The RG network was generated using the Erdős–Rényi model $G(N, p)$ with an edge probability $p \approx 8/49999$, ensuring an average degree close to 8. The SF network followed the Barabási Albert model with $m = 4$ and formed hubs through preferential attachment. The I2P Prime (I2P') network combined a small-world base with additional edges created through a hybrid process simulating preferential attachment and random long-range connections. This design aimed to emulate the dynamic nature and global reach in the actual I2P (Garlic) network topologies. The core simulation logic is formalized in Algorithm 1, which outlines the progressive removal of nodes and evaluation of key resilience metrics at each step.

Algorithm 1 Resilience Evaluation via Progressive Node Removal

Graph G, strategy $S \in \{\text{random}, \text{degree}, \text{betweenness}\}$ Metrics per step: LCC size, components, path length, clustering **for** each step $t = 1$ to 100 **do** Identify and remove top 1% nodes from G based on S Extract largest connected component (LCC) Compute: number of components, LCC size, avg. path length, clustering coefficient Store metrics for step t **return** Time-series of resilience metrics

This procedure was applied independently to each of the three network models under all three attack strategies, generating time-series data for structural degradation analysis. Each network's nodes represent I2P routers, and edges represent encrypted tunnels. After generating the networks, we computed key baseline metrics: the number of connected components, the size of the largest connected component (LCC), the average shortest path length, the clustering coefficient, and the estimated network diameter. We then conducted percolation-based failure simulations under two main scenarios: (1) Random Failures (Stochastic Percolation), at each step 1% of nodes were randomly removed to mimic hardware failures, churn, or unplanned node exits; (2) Targeted Attacks (Adversarial Percolation), at each step 1% of nodes with the highest degree or betweenness centrality were removed, with node metrics recalculated dynamically after each step to reflect structural changes. This progressive removal continued in 1% increments until the network was entirely dismantled. At each stage, we measured the same key resilience metrics to observe structural degradation. Particular attention was paid to the size and persistence of the LCC, as its decline marks a critical loss of global connectivity.

To support the simulations, we calculated theoretical percolation thresholds. For random failures, the expected critical fraction is given by:

$$f_c^{\text{random}} = 1 - \frac{1}{\langle k \rangle}$$

For targeted attacks, the collapse point was estimated using the second moment of the degree distribution:

$$f_c^{\text{targeted}} \approx \frac{\langle k^2 \rangle - \langle k \rangle}{\langle k \rangle \cdot \langle k^2 \rangle}$$

These simulations enabled a comparative resilience analysis of the three network models under both accidental and adversarial threats, offering empirical insight into how I2P's architecture influences its robustness in real-world conditions.

4 | RESULTS

We evaluated the resilience of the three network models, Random Graph (RG), Scale-Free (SF), and I2P Prime, each consisting of 50,000 nodes. All networks began as fully connected structures, with the I2P Prime model exhibiting higher clustering and

slightly longer path lengths, reflecting its hybrid and preferential topology. The goal was to assess how each network deteriorates under random failures and targeted attacks using degree and betweenness centrality strategies.

Figure 2 shows the evolution of the largest connected component (LCC) and the number of network components as nodes are progressively removed. Under random node removal, all models degrade gradually, with I2P Prime retaining structural integrity well beyond 60% node loss. Targeted removals based on degree or betweenness metrics lead to accelerated fragmentation, particularly in the SF network, which collapses before reaching 40% removal. The RG network performs slightly better but still loses global connectivity much earlier than I2P Prime. Notably, the I2P Prime model withstands both targeted attacks more effectively, with a slower decline in LCC size and a delayed rise in disconnected components.

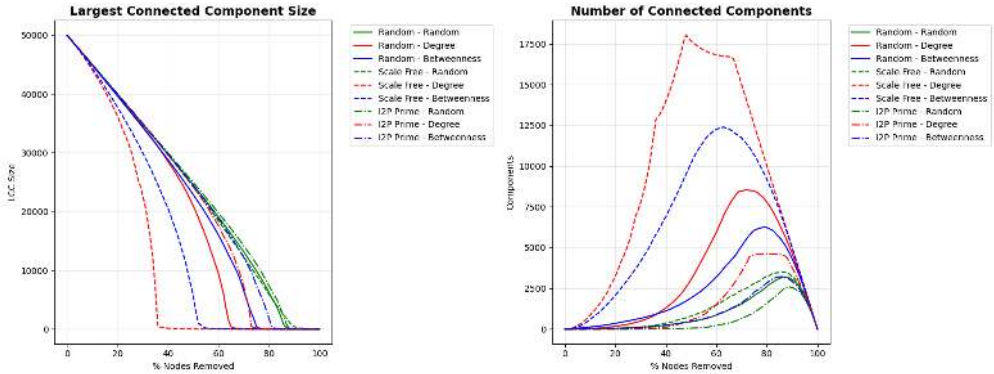

FIGURE 2 Impact of node removal on (left) Largest Connected Component (LCC) size and (right) number of connected components across RG, SF, and I2P Prime networks under three attack strategies.

Figure 3 presents two additional resilience indicators: average shortest path length and clustering coefficient. Random failures result in minimal changes to average path lengths. In contrast, targeted attacks on SF and RG networks lead to abrupt increases in path length, peaking around 60 hops before the networks disintegrate. I2P Prime, however, experiences smoother increases, even under attack, suggesting more distributed and fault-tolerant routing paths. The clustering coefficient remains stable for I2P Prime during random removals and only gradually decreases under targeted attacks. SF and RG models exhibit sharp drops in clustering, indicating a loss of local neighborhood cohesion.

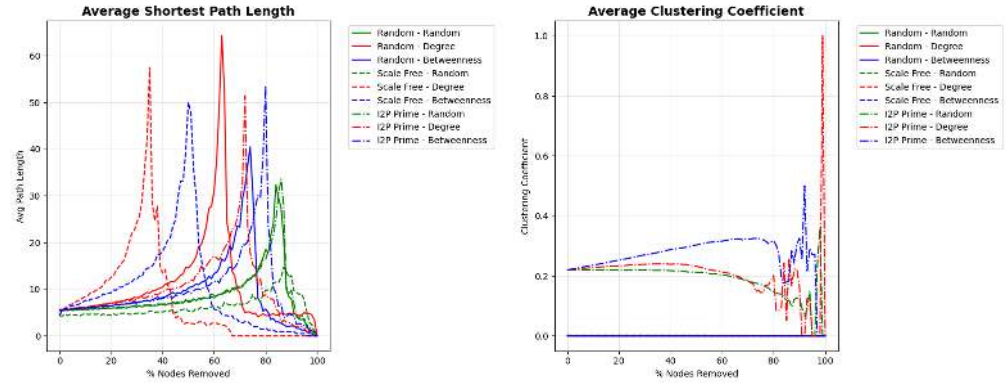

FIGURE 3 Average shortest path length (left) and clustering coefficient (right) under progressive node removals. I2P Prime shows greater tolerance to disruption, preserving structural properties longer than SF and RG.

Figure 4 summarizes two key resilience metrics across all networks and attack types. The left panel shows normalized resilience scores calculated as the area under the LCC curve (AUC). I2P Prime achieves the highest resilience scores in all three attack scenarios. SF scores lowest, particularly under degree-based attacks, confirming its vulnerability due to centralized hub structures. The right panel illustrates the critical failure point, thus, the percentage of nodes that must be removed to reduce the LCC below 50% of its original size. I2P Prime requires nearly 50% removal under all conditions, while SF collapses after losing just 28% of its most connected nodes.

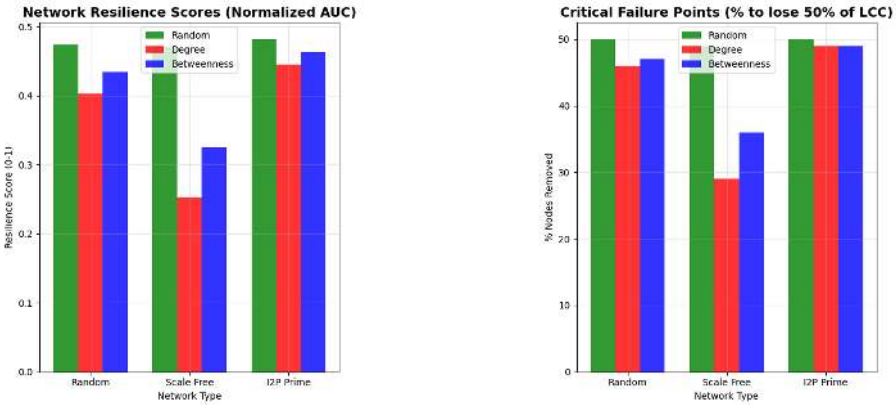

FIGURE 4 (Left) Normalized network resilience scores based on area under LCC curve. (Right) Critical failure thresholds for losing 50% of LCC. I2P Prime demonstrates superior robustness in both metrics.

Overall, I2P Prime consistently outperforms traditional random and scale-free models under stochastic and adversarial failures. Its structural balance incorporates clustering, redundancy, and partial preferential attachment. This results into slower degradation, higher tolerance to attacks, and preservation of network coherence even under extreme failures.

5 | DISCUSSION AND CONCLUSION

This study demonstrates that the I2P Prime model offers significantly greater resilience than Random Graph (RG) and Scale-Free (SF) topologies. Under random failures, all network models retained large connected components. I2P Prime consistently outperformed RG and SF in preserving connectivity, maintaining shorter paths, and sustaining clustering structure even after 60% node loss. These findings indicate that the real (live) I2P network as suspected to be (I2P prime) in this study, is robust against uncoordinated failures such as churn, outages, or voluntary disconnections. Under adversarial conditions, resilience patterns diverged sharply. The SF network collapsed rapidly when only 25–35% of high-degree or high-betweenness nodes were removed, confirming its vulnerability to targeted attacks. RG showed moderate fragility. In contrast, I2P Prime resisted fragmentation until nearly 50% of the most critical nodes were removed, indicating a more fault-tolerant structure. Its slower LCC decline, smoother path length increase, and delayed component explosion confirm that no single subset of nodes dominates global connectivity.

These results reveal two important implications. First, I2P's structural design benefits from decentralizing critical paths. Clustering, peer diversity, and geographic bias in peer selection reduce reliance on hubs, distributing risk across the network. Second, resilience can be further improved by adopting dynamic routing strategies, such as periodic peer shuffling, load-aware edge formation, or rotating tunnels, that minimize long-lived bottlenecks and prevent adversaries from targeting persistent bridges and nodes.

From a security and policy perspective, the findings underscore that while I2P is resilient to random failures, strategic disruption by a well-informed actor could severely impair anonymity and communication. Selective router (node) takedowns can fragment the network and increase traffic visibility on remaining nodes, raising the risk of deanonymization. Therefore, defensive design must preserve privacy under normal operation and resist targeted structural degradation.

In conclusion, our empirical analysis shows that resilience in anonymity networks depends not just on decentralization but also on the topology's internal organization. I2P Prime (the proposed topology for the Garlic (I2P) network) demonstrates structural balance combining clustering, randomness, and adaptive growth, and can support both privacy and robustness.

Future enhancements to I2P should leverage these insights to build an overlay that resists attack without sacrificing efficiency or anonymity.

6 | LIMITATIONS AND FUTURE WORK

While this study presents a comprehensive resilience analysis of three network modelling I2P, several limitations should be acknowledged. First, the simulation environment models all links as uniformly weighted and does not fully capture real-world variability such as asymmetric bandwidth, latency fluctuations, or cryptographic processing delays inherent to garlic routing. These factors may influence how the I2P network degrades or recovers under failures. Second, node churn, a defining feature of the live I2P network, is not dynamically modeled. Routers frequently join and leave the network, affecting route stability, tunnel rebuilding, and long-term connectivity. Our large-scale snapshots may not entirely reflect the temporal fluidity of I2P's topology. Third, targeted attack simulations assume adversaries have perfect, real-time knowledge of node centrality metrics. Such precision is difficult to obtain without extensive surveillance or compromised vantage points. Incorporating partial, delayed, or probabilistic knowledge models would yield a more realistic view of adversarial capabilities. Centrality calculations, particularly betweenness, required approximations to maintain tractability. These approximations may slightly affect results near collapse thresholds, but they do not alter the observed patterns. Using 50,000-node strongly mitigates the study's limitations, mirroring I2P's estimated scale.

Future research should extend the model by introducing dynamic churn mechanisms that simulate node volatility and allow assessment of I2P's self-healing properties after partial fragmentation. Exploring resilience under resource-constrained adversaries with incomplete topological awareness would also be valuable, emulating more realistic threat actors. Finally, empirical validation using live I2P data such as topology snapshots, latency probing, or tunnel path sampling will be crucial for grounding the simulation in observable behavior and refining resilience strategies for deployment in production environments.

REFERENCES

1. Bou Abdo J, Hossain L. Modeling the Invisible Internet. In: International Conference on Complex Networks and Their Applications. Springer. 2023:359–370.
2. Edman M, Yener B. On anonymity in an electronic society: A survey of anonymous communication systems. *ACM Computing Surveys (CSUR).* 2009;42(1):1–35.
3. Amalou W, Mehdi M. Anonymous Traffic Detection and Identification. In: 2023 International Conference on Advances in Electronics, Control and Communication Systems (ICAECCS). IEEE. 2023:1–5.
4. Paphitis A, Kourtellis N, Sirivianos M. Resilience of blockchain overlay networks. In: International Conference on Network and System Security. Springer. 2023:93–113.
5. Baraz A, Montasari R. Law enforcement and the policing of cyberspace. In: , , Digital Transformation in Policing: The Promise, Perils and Solutions. Springer, 2023:59–83.
6. Chao D, Xu D, Gao F, Zhang C, Zhang W, Zhu L. A Systematic Survey On Security in Anonymity Networks: Vulnerabilities, Attacks, Defenses, and Formalization. *IEEE Communications Surveys & Tutorials.* 2024.
7. Maalavika S, Thangavel G, Basheer S. A Review on Garlic Routing and Artificial Intelligence Applications in Public Network. In: 2023 International Conference on Computer Science and Emerging Technologies (CSET). IEEE. 2023:1–6.
8. Sousa dA. Improving the connectivity resilience of a telecommunications network to multiple link failures through a third-party network. In: 2020 16th International Conference on the Design of Reliable Communication Networks DRCN 2020. IEEE. 2020:1–6.
9. Albert R, Jeong H, Barabási AL. Error and attack tolerance of complex networks. *nature.* 2000;406(6794):378–382.
10. Barabási AL, Bonabeau E. Scale-free networks. *Scientific american.* 2003;288(5):50–9.
11. Zhao JH, Zhou HJ, Liu YY. Inducing effect on the percolation transition in complex networks. *Nature communications.* 2013;4(1):2412.
12. Gao J, Barzel B, Barabási AL. Universal resilience patterns in complex networks. *Nature.* 2016;530(7590):307–312.
13. Mohammad GB, Shitharth S, Dileep P. Classification of Normal and Anomalous Activities in a Network by Cascading C4. 5 Decision Tree and K-Means Clustering Algorithms. *Social Network Analysis: Theory and Applications.* 2022:109–131.
14. Huang Z, Wang C, Ruj S, Stojmenovic M, Nayak A. Modeling cascading failures in smart power grid using interdependent complex networks and percolation theory. In: 2013 IEEE 8th Conference on Industrial Electronics and Applications (ICIEA). IEEE. 2013:1023–1028.
15. Arora A, Garman C. Improving the Performance and Security of Tor's Onion Services. *Proceedings on Privacy Enhancing Technologies.* 2025.
16. De Boer T, Breider V. Invisible internet project (I2P). *System and Network Engineering.* 2019:1–16.
17. Magán-Carrión R, Abellán-Galera A, Maciá-Fernández G, García-Teodoro P. Unveiling the I2P web structure: A connectivity analysis. *Computer Networks.* 2021;194:108158.
18. Gaarder A. Routing for a dark net overlay network. Master's thesis. NTNU. 2023.
19. Ding J, Ma Z, Wu Y, Xu J. Efficient random graph matching via degree profiles. *Probability Theory and Related Fields.* 2021;179:29–115.
20. Broido AD, Clauset A. Scale-free networks are rare. *Nature communications.* 2019;10(1):1017.
21. Muntaka SA, Bou Abdo J, Akanbi K, et al. Mapping the Invisible Internet: Framework and Dataset. 2025