Identification of Authoritative Nodes and Dismantling of Illicit Networks Using a Novel Metric for Measuring Strength of a Graph

Kartikeya Kansal and Arunabha Sen

School of Computing and Augmented Intelligence, Arizona State University, Tempe, 85048 AZ USA,
kkansal1@asu.edu, asen@asu.edu,

Abstract. Dismantling criminal networks, containing epidemics, or mitigating misinformation through selective node removal is a well-studied challenge. Evaluating such efforts requires measuring network *strength* before and after node removal. A process P_1 is more effective than P_2 if the residual network after removing k nodes via P_1 is weaker than that of P_2. Most existing metrics rely purely on *structural* properties (e.g., connectivity, component size) and ignore how practitioners, especially in law enforcement, perceive network robustness. These perceptions often diverge significantly from topology-driven assessments. We propose a novel strength metric that integrates both structural features and *human perception*. By collecting perceptual feedback via surveys on synthetic and real-world networks, we derive a tunable weight vector capturing perceived importance of connected components. Experiments show our metric aligns more closely with human judgment than traditional methods and improves identification of *authoritative nodes* for effective dismantling.

Keywords: Network Strength Metric, Graph Fragmentation, Authoritative Node Identification, Human-Centric Network Analysis

1 Introduction

Targeted dismantling of covert networks, criminal, terrorist, or informational, has long been an active research problem. The objective is to identify nodes whose removal most significantly weakens the network [1], [2]. Foundational studies adopt either a network science approach [3], [4] or a graph-theoretic optimization perspective [5]. Despite methodological diversity, most strategies ultimately require comparing the strength of a network before and after node removal.

Classical notions of strength, such as Gusfield's connectivity metric [6] or Chvátal's toughness [7] quantify resilience based solely on structural disruption. Similarly, Girvan and Newman's edge betweenness centrality [8] and spectral robustness metrics [9] analyze graph topology but remain difficult to interpret in operational settings. Metrics like the Graph Fragmentation Problem (GFP) [10] and Cole's models [5] have been widely used but consistently fail to capture how law enforcement agents or field experts perceive network degradation.

This gap is especially critical in real-world contexts. Covert networks, such as terrorist or smuggling groups, are typically small to medium in scale, far from massive social graphs like Facebook or Google datasets, making human evaluation both feasible and meaningful. Importantly, while human perception may carry biases, it is ultimately humans who make dismantling decisions in practice. Therefore, a metric that integrates human judgment with structural properties provides a more realistic and actionable view of network resilience.

Our work introduces a *perception-aware* strength metric that generalizes purely structural approaches by adding a tunable weight vector W, derived from human surveys on synthetic and real covert networks. Unlike previous metrics, it bridges algorithmic evaluations with how domain experts intuitively assess robustness, addressing a critical usability gap in law enforcement and epidemic response scenarios.

Key Contributions:

- A novel strength metric combining structural topology and human perception, mitigating the disconnect between theory and field practice.
- A survey-driven procedure to compute weight vectors capturing perceived importance of component sizes.
- Validation on synthetic and real criminal networks, demonstrating superior alignment with human consensus compared to Cole 1, Cole 2, and GFP.
- Clarification of scope: our metric is designed for small-to-medium networks, where human evaluation is feasible, rather than very large-scale social graphs.

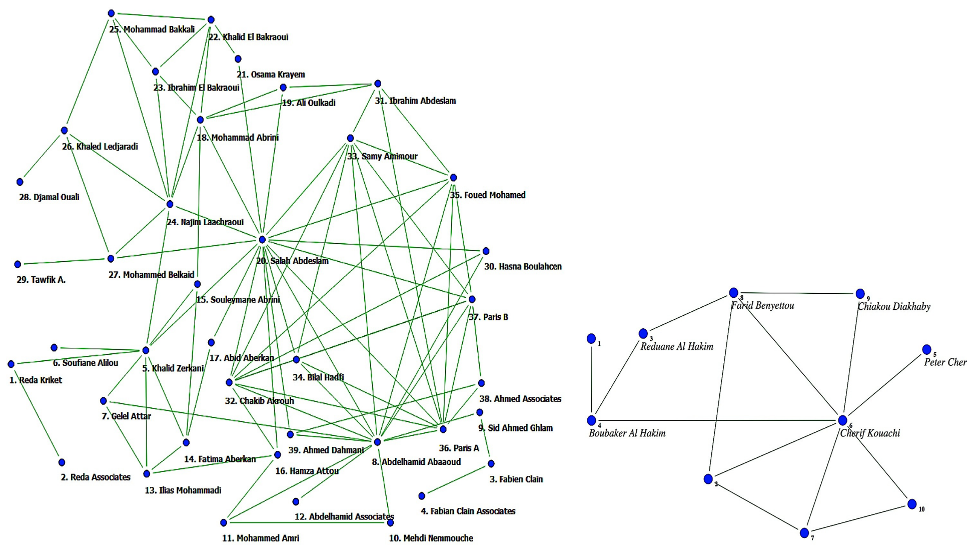
Figure 1 shows an example network used in our evaluation, representing the Paris 2015 terrorist network.

2 Proposed Strength Metric

Existing approaches to measuring network strength rely solely on structural topology, overlooking how human agents perceive robustness. Our metric explicitly integrates both structural information and human perception.

A graph $G = (V, E)$ may have one or more connected components. Let $|V| = n$ and the graph be composed of k components $C_1, \ldots, C_k$, with $\sum_{i=1}^{k} |C_i| = n$. We define the *Connected Component Size Distribution* (CCSD) of G as a vector $[nc_1, nc_2, \ldots, nc_n]$, where nc_i denotes the number of components of size i. For a fully connected graph of n nodes, CCSD is $[0, \ldots, 0, 1]$.

While larger components generally imply higher robustness, their perceived importance varies across domains. To account for this, we associate a weight w_i with a component of size i, forming a *weight vector* $W = [w_1, \ldots, w_n]$. This vector captures human perception of network resilience, derived from user studies (detailed in Section 3.2).



(a) IS-Europe Zerkani Network

(b) Paris Network

Fig. 1: Example of a covert network (Paris Bataclan attack, 2015).

Using CCSD and W, we define the network strength metric:

$$\sigma(G, W) = \sum_{i=1}^{n} i \times w_i \times nc_i.$$

For a connected graph, $\sigma(G, W) = n \times w_n$. This formulation generalizes traditional structural metrics and allows perception-aware evaluation of network resilience and fragmentation.

We use this metric both to (i) quantify the strength of a network and (ii) guide the identification of k most authoritative nodes. The second application involves an ILP formulation that has been archived and is omitted for brevity [11].

3 Data Collection and Weight Computation

3.1 Graphs for Experiments

To derive perception-based weights, we created a diverse pool of networks. Approximately 150 synthetic graphs were generated using `erdos_renyi_graph` and `gnm_random_graph` models in NetworkX, varying from 3 to 50 nodes. Edge density was controlled via $p \in [0.05, 0.5]$ for Erdős–Rényi graphs, while $G(n, m)$ graphs allowed fixed edge counts.

We also incorporated real-world covert networks, including Saxena Terror India [12], Rhodes Bombing [13], Global Suicide Attacks [14], Cocaine Dealing

[15], ACERO Smuggling [16], Human Trafficking (CHIAPAS) [17], and Paris/Zerkani networks (Figure 1). Around 120 graphs were used to compute weight vectors, and the rest for evaluation.

3.2 Human-Perception Study

To align the metric with human intuition, we conducted a user study with 50 participants. Each participant evaluated the perceived "strength" of synthetic and real networks on a normalized scale $[1, n]$, where n is the node count. Sparse, fragmented graphs were typically rated as weak, while dense cohesive graphs scored higher.

Responses for each graph were averaged to yield a ground-truth perception score. Figure 2 shows examples of graphs presented to participants.

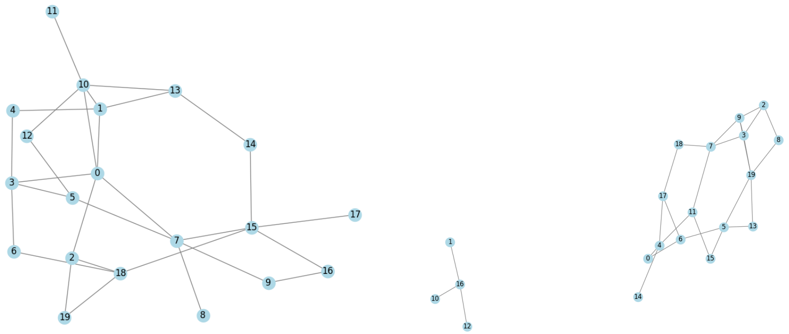


Fig. 2: Example survey graphs shown to participants to capture perceived strength.

3.3 Weight Vector Estimation

Given m networks G_j with human-estimated scores E_j, we express:

$$E_j = \sum_{i=1}^{n} i \times w_i \times nc_i(G_j).$$

This yields a system of m linear equations with unknown weights w_i. We solved it via least-squares regression, producing a stable weight vector $\hat{W}$ that minimizes deviation from human ratings.

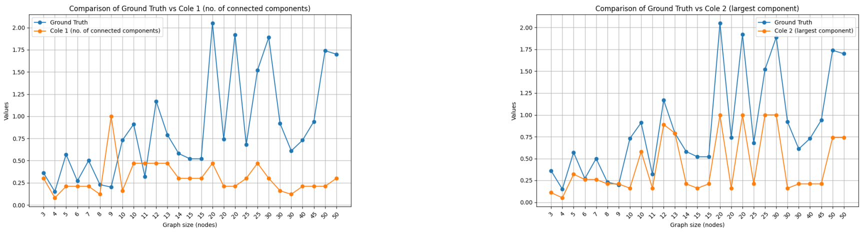
The resulting weights reflect the perceived importance of different component sizes. Smaller components were assigned lower influence, while larger components (reflecting more cohesive substructures) received higher weights. These optimized weights inform all subsequent strength evaluations and node-importance analyses.

4 Experimental Evaluation of the Proposed Metric

We validated the proposed metric by comparing it with three baselines: **Cole 1** (component count), **Cole 2** (largest component size), and **GFP** (attack score model). Ground Truth was defined as the average human-perceived strength from surveys.

4.1 Network Strength Evaluation

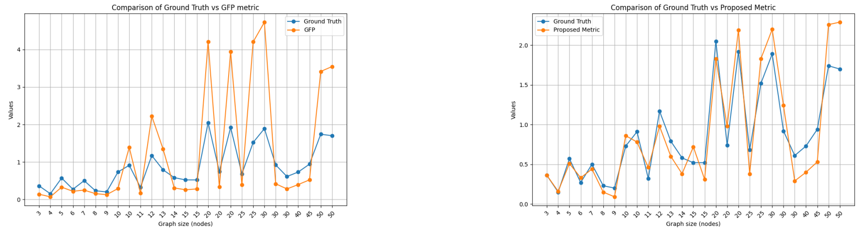
Synthetic Graphs Synthetic networks generated via Erdős–Rényi and $G(n, m)$ models (Section 3.1) were evaluated using all metrics. Figure 3 and 4 shows representative results. Cole 1 consistently underestimated medium–large graphs, Cole 2 under-scaled for dense graphs, and GFP frequently overestimated strength. In contrast, the proposed metric closely followed Ground Truth across all node sizes, adapting better to varying connectivity patterns.



(a) Comparison of Ground Truth and Cole 1 (Based on the Number of Connected Components).

(b) Comparison of Ground Truth and Cole 2 (Based on the Size of the Largest Component).

Fig. 3: Comparison between Ground Truth and Cole methods using two different metrics (synthetic graphs).



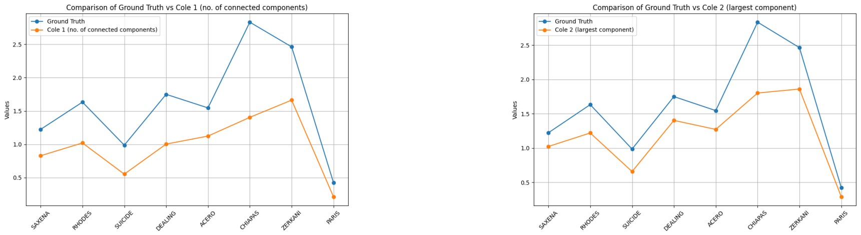
(a) Comparison of Ground Truth and the GFP paper Metric.

(b) Comparison of Ground Truth and the Proposed Metric.

Fig. 4: Comparison of Ground Truth against GFP and Proposed metrics (synthetic graphs).

We quantified alignment with Root Mean Squared Error (RMSE). As shown in Table 1, the proposed metric achieved the lowest error (0.26), outperforming Cole 1 (0.81), Cole 2 (0.55), and GFP (1.08).

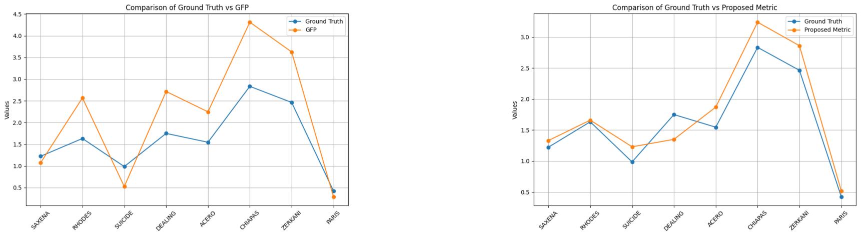
Real-World Networks Similar experiments on covert networks (e.g., Chiapas, Paris, Zerkani) confirmed the same pattern. Cole 1 showed mild underestimation on structured networks, while GFP again overestimated strength. The proposed metric remained closest to human judgment, effectively capturing both typical and outlier cases (Figure 5 and 6).



(a) Comparison of Ground Truth and Cole 1 (Based on the Number of Connected Components).

(b) Comparison of Ground Truth and Cole 2 (Based on the Size of the Largest Component).

Fig. 5: Comparison between Ground Truth and Cole's metrics (real-world networks).



(a) Comparison of Ground Truth and the GFP paper Metric.

(b) Comparison of Ground Truth and the Proposed Metric.

Fig. 6: Comparison of Ground Truth against GFP and Proposed metrics (real-world networks).

Across all graphs, the proposed metric achieved the lowest RMSE (0.29) compared to Cole 1 (0.72), Cole 2 (0.49), and GFP (0.87), highlighting its generalizability to both synthetic and real datasets.

4.2 Identifying Authoritative Nodes

We also evaluated how well each metric identified the most influential nodes ($k = 1, 2$). For each real network, participants selected the top 1 and top 2

Metric	**Synthetic RMSE**	**Real RMSE**
Proposed Metric	**0.26**	**0.29**
Cole 1	0.81	0.72
Cole 2	0.55	0.49
GFP	1.08	0.87

Table 1: RMSE comparison between Ground Truth and competing metrics.

authoritative nodes. Predictions from all metrics were compared against these survey-based ground truths.

Our metric achieved the highest agreement. For **single-node** selection, Exact Match was **0.75** vs. 0.5 (Cole 1) and 0.38 (GFP), with 61% alignment in percentage match. For **two-node** selection, Exact Match was **0.38** vs. 0.25 for all baselines.

Metric	**Exact Match (1 node)**	**Exact Match (2 nodes)**	**% Match**
Proposed Metric	**0.75**	**0.38**	**61.3**
Cole 1	0.50	0.25	54.6
Cole 2	0.38	0.25	47.6
GFP	0.38	0.25	47.6

Table 2: Authoritative node identification vs. human ground truth.

Unlike structural baselines, our metric consistently aligned with human intuition, especially in covert networks where perceived influence differs from pure topological centrality.

4.3 Summary

Across all experiments, **Cole 1 & 2** lacked sensitivity to larger cohesive structures. **GFP** overestimated resilience, particularly in fragmented topologies. The **Proposed Metric** had the lowest RMSE, best agreement with human surveys, and superior identification of critical nodes. These results validate the practical value of incorporating human perception into network strength modeling.

5 Conclusion

We introduced a novel *perception-aware* metric for measuring network strength that combines structural topology with human intuition, addressing gaps in traditional approaches. Unlike purely topological methods, our approach reflects how humans, such as law enforcement agents, assess network resilience in real scenarios. While perceptions may vary, averaging across participants mitigates bias and yields a consensus ground truth aligned with practical actionability.

Our work targets small to medium-scale covert networks, such as terrorist or trafficking groups, where human evaluation is feasible and relevant. Large-scale social graphs like Facebook lie beyond the current scope. We did not compare with all centrality measures, as they fall within the same class of structural metrics (e.g., Cole, GFP). Instead, we show that incorporating human perception provides an orthogonal advantage over any purely structural approach.

Across synthetic and real-world networks, the proposed metric achieved the lowest RMSE against human ground truth and higher accuracy in identifying authoritative nodes, validating its utility in high-stakes scenarios. Future work will extend this approach to dynamic networks, study variability in human responses, and explore incorporating additional structural features such as link density or clustering.

References

1. Kempe, D., Kleinberg, J., Tardos, E.: Maximizing the spread of influence through a social network. In: Proceedings of the Ninth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pp. 137–146 (2003)
2. Ren, X.-L., Gleinig, N., Helbing, D., Antulov-Fantulin, N.: Generalized network dismantling. Proceedings of the National Academy of Sciences **116**(14), 6554–6559 (2019)
3. Lu, L., Chen, D., Ren, X.-L., Zhang, Q.-M., Zhang, Y.-C., Zhou, T.: Vital nodes identification in complex networks. Physics Reports **650**, 1–63 (2016)
4. Albert, R., Jeong, H., Barabasi, A.-L.: Error and attack tolerance of complex networks. Nature **406**(6794), 378–382 (2000)
5. Shen, S., Smith, J.C., Goli, R.: Exact interdiction models and algorithms for disconnecting networks via node deletions. Discrete Optimization **9**(3), 172–188 (2012)
6. Gusfield, D.: Computing the strength of a graph. SIAM Journal on Computing **20**(4), 639–654 (1991)
7. Chvatal, V.: Tough graphs and Hamiltonian circuits. Discrete Mathematics **5**(3), 215–228 (1973)
8. Girvan, M., Newman, M.E.J.: Community structure in social and biological networks. Proceedings of the National Academy of Sciences **99**(12), 7821–7826 (2002)
9. Chung, F.R.K.: Spectral Graph Theory. CBMS Regional Conference Series in Mathematics, vol. 92. American Mathematical Society, Providence (1997)
10. Piccini, J., Robledo, F., Romero, P.: Graph Fragmentation Problem. In: ICORES, pp. 137–144 (2016)
11. Kansal, K., Sen, A.: Identification of Authoritative Nodes and Dismantling of Illicit Networks Using a Novel Metric for Measuring Strength of a Graph https://arxiv.org/abs/2507.12711 (2025)
12. Saxena, S., Santhanam, K., Basu, A.: Application of social network analysis (SNA) to terrorist networks in Jammu & Kashmir. Strategic Analysis **28**(1), 84–101 (2004)
13. Rhodes, C.J., Jones, P.: Inferring Missing Links in Partially Observed Social Networks. Journal of the Operational Research Society **60**, 1373–1383 (2009)
14. Acosta, B., Childs, S.J.: Illuminating the global suicide-attack network. Studies in Conflict & Terrorism **36**(1), 49–76 (2013)
15. Natarajan, M.: Understanding the Structure of a Large Heroin Distribution Network: A Quantitative Analysis of Qualitative Data. Journal of Quantitative Criminology **22**(2), 171–192 (2006).
16. Jimenez-Salinas Framis, A.: Illegal networks or criminal organizations: Power, roles and facilitators in four cocaine trafficking structures. In: Third Annual Illicit Networks Workshop, Montreal, Canada (2011).
17. De la Mora Tostado, S., Hernandez-Vargas, E.A., Nunez-Lopez, M.: Modeling human trafficking and the limits of dismantling strategies. Social Network Analysis and Mining **14**(1), 84 (2024)