Review of: "Protection of Complex Network Systems From Targeted Attacks and Non-Target Lesions"

Jamal El Kafi[1]

1 Université Chouaib Doukkali

Potential competing interests: No potential competing interests to declare.

Review article by *Pr. Jamal EL KAFI*:

Protection of Complex Network Systems From Targeted Attacks and Non-Target Lesions

I. **Analysis of the Abstract**

The abstract provides a good starting point for the article. Here's a breakdown of its strengths and areas for improvement :

a. **Strengths :**

- Clearly states the topic : Vulnerability of complex network systems (NS)
- Mentions both structural and flow approaches for analysis
- Highlights different types of attacks (targeted and non-targeted)
- Briefly describes the methodology (scenarios and comparisons)
- Emphasizes the key finding : flow approach offers a more realistic picture

a. **Areas for Improvement:**

- **Specificity :**

  - Consider replacing "various types" with specific examples of targeted attacks and non-targeted lesions (e.g., malware attacks, power outages).
  - Briefly mention the criteria used to identify "most important" system elements.
  - Can you elaborate on the "scale" of system lesions ?

- **Focus on Qeios Audience :**

  - Qeios emphasizes interdisciplinary research. Can you hint at the broader implications of your findings beyond the specific field of network science?

a. **Here's an example of a revised abstract incorporating these suggestions :**

This study conducts a comparative analysis of structural and flow approaches to assess the vulnerability of complex network systems (NS) to targeted attacks (e.g., malware) and non-targeted disruptions (e.g., power outages). We explore

scenarios of both sequential attacks on critical elements (identified by centrality measures) and coordinated strikes on multiple key network components. The analysis investigates how the scale of system damage arising from diverse negative influences differs between these approaches. Our results demonstrate that the flow approach provides a more realistic picture of such disruptions and that attack strategies based on network flow models can be more effective in targeting vulnerabilities. This research contributes to enhanced network resilience across various disciplines by offering a deeper understanding of how network structure and information flow interact under attack scenarios.

This revised version provides more specific details, highlights the interdisciplinary value of your research, and better aligns with the potential interests of the Qeios audience.

I. **Analysis of the Introduction Section**

The introduction provides a good overview of the topic and motivates the need for a flow-based approach. Here's a breakdown of its strengths and areas for improvement:

a. **Strengths :**

- Clearly establishes the relevance of the research by citing real-world examples (pandemic, war).
- Highlights limitations of the structural approach to vulnerability analysis.
- Introduces the concept of "flow approach" and its potential benefits.

a. **Areas for Improvement :**

- **Focus and Conciseness :**
  - The introduction could be more concise, particularly the first paragraph. Consider removing references to specific events (Covid-19, Ukraine war) and focus on the broader concept of targeted attacks and non-targeted disruptions on complex systems.
  - Streamline the discussion of lesion types (local, group, etc.).
- **Clarity and Flow :**
  - The connection between the real-world examples and the limitations of the structural approach could be strengthened.
  - Consider restructuring the paragraph on the limitations of the structural approach. You could separate the discussion of attack scenarios and lesion scale into two points for better clarity.
- **Highlight Qeios Focus :** Briefly mention how your research contributes to a broader understanding beyond network science (e.g., implications for system resilience across disciplines).

a. **Here's an example of a revised introduction incorporating these suggestions:**

The increasing interconnectedness of complex systems across various disciplines makes them vulnerable to diverse disruptions, both targeted attacks and non-targeted events. The limitations of current approaches, which primarily focus on network structure for vulnerability analysis, become apparent when considering real-world scenarios. For instance, the

structural approach might underestimate the cascading effects of disruptions that propagate through the system's operational processes. Additionally, existing methods may not fully capture the true extent of damage caused by such disruptions.

This article proposes a flow-based approach to vulnerability analysis of complex network systems (NS). This approach focuses on information flow within the network to assess the impact of disruptions and optimize mitigation strategies. We argue that the flow approach offers a more comprehensive understanding of system vulnerability compared to the structural approach, particularly when evaluating real-world losses and designing effective countermeasures.

I. **Analysis of Section 2 "Attacks on the structure of network system"**

This section provides a detailed explanation of attacks on network system structure. Here's a breakdown of its strengths and areas for improvement:

a. **Strengths :**

- Clearly defines the limitations of centrality-based approaches for identifying critical nodes.
- Introduces different types of targeted attacks (sequential, simultaneous) and non-targeted lesions.
- Describes various scenarios for attack implementation based on centrality and k-core concepts.

a. **Areas for Improvement :**

- **Focus and Conciseness :**
  - The section could benefit from being more concise. Consider streamlining the explanation of centrality measures and their limitations.
  - Focus on the key message: structural approaches underestimate the impact of disruptions by neglecting information flow.
- **Clarity and Flow :**
  - The connection between different types of attacks and their implications for scenario development could be strengthened.
  - Consider restructuring the section to improve readability. You could separate the discussion of centrality measures, attack types, and scenario development into distinct subsections with clear headings.
- **Highlight Qeios Focus:** Briefly mention how this analysis of structural limitations paves the way for the introduction of the flow-based approach in the next section.

a. **Here's an example of a revised section incorporating these suggestions :**

2. Limitations of Structural Approaches to Network Vulnerability

While centrality measures offer a valuable tool for identifying critical nodes in network systems, they have limitations when

assessing vulnerability to disruptions. These measures primarily focus on network structure and neglect the flow of information or resources within the system. This can lead to underestimating the impact of attacks that target specific pathways or disrupt information flow.

This section explores different types of targeted attacks (sequential, simultaneous) and non-targeted disruptions. We discuss how these attacks can unfold and the limitations of structural approaches in capturing their full impact. We then introduce various scenarios for attack implementation based on centrality and k-core concepts. These scenarios highlight the need for a more comprehensive approach that considers information flow alongside network structure.

This analysis paves the way for the introduction of the flow-based approach in the next section, which offers a more holistic understanding of network vulnerability by incorporating information flow dynamics.

I. **Analysis of Section 3 "Attacks on operation process of network system**

This section effectively introduces the flow-based approach to network vulnerability analysis. Here's a breakdown of its strengths and areas for improvement:

a. **Strengths :**

- Clearly defines the flow model and its advantages over the structural model.
- Introduces flow-based centrality measures for identifying functionally important nodes.
- Demonstrates the flow approach's ability to capture cascading effects of disruptions.
- Compares the flow and structural approaches through figures, highlighting the broader impact zone identified by the flow model.

a. **Areas for Improvement :**

- **Focus and Conciseness :**
  - Consider streamlining the explanation of flow model details (e.g., V(t) matrix definition).
  - Focus on the key message: flow approach provides a more comprehensive picture of disruption impact by considering information flow.
- **Clarity and Flow :**
  - Consider restructuring the section for better readability. Separate the introduction of the flow model, flow-based centrality measures, and the comparison with the structural approach into distinct subsections with clear headings.
- **Highlight Qeios Focus :**
  - Briefly mention how the flow-based approach contributes to broader disciplines beyond network science (e.g., implications for system resilience across domains).

a. **Here's an example of a revised section incorporating these suggestions:**

3. Flow-Based Approach to Network Vulnerability Analysis

The limitations of centrality measures based solely on network structure become apparent when considering disruptions that target information flow within the system. To address this, we propose a flow-based approach to network vulnerability analysis.

This approach utilizes a flow model that captures the movement of information or resources through the network. By analyzing this flow, we can identify functionally important nodes based on their role as generators, receivers, or transit points for information flow. Flow-based centrality measures, such as input/output strength and betweenness, are introduced to quantify this functional importance.

A key advantage of the flow-based approach is its ability to capture cascading effects of disruptions. Unlike the structural approach, which only considers directly affected nodes, the flow model reveals how disruptions can propagate through the network, impacting even seemingly distant elements. This is demonstrated in the figures accompanying this section, where the flow approach identifies a significantly larger zone of consequentially injured nodes compared to the structural approach.

This broader picture of disruption consequences allows for more effective mitigation strategies. By identifying critical flow paths and potential bottlenecks, we can prioritize protection efforts on the most functionally important components of the network system.

The flow-based approach, with its focus on information flow dynamics, has implications beyond network science. It contributes to a more holistic understanding of system resilience across various disciplines by providing a framework for analyzing how disruptions propagate and impact system functionality.

I. **Analysis of Section 4 “Optimization of targeted attack scenarios”**

This section explores optimization strategies for targeted attacks on network systems. Here's a breakdown of its strengths and areas for improvement:

a. **Strengths:**

- Introduces the concept of flow-based cores (λ-cores) for identifying critical attack targets.
- Demonstrates the advantage of λ-cores over structural k-cores in minimizing the number of attack targets while achieving maximum disruption.
- Briefly mentions network granulation (edge blocking) as a potential attack strategy.

a. **Areas for Improvement:**

- **Focus and Neutrality:**
    - The section's focus on real-world examples with military applications might not be suitable for a broader audience. Consider using neutral language and hypothetical scenarios.

- Avoid glorifying or justifying attacks. The focus should be on the effectiveness of flow-based methods for understanding vulnerabilities, not on specific attack strategies.

- **Clarity and Organization:**
  - Consider restructuring the section to improve readability. Separate the introduction of λ-cores, the comparison with k-cores, and the discussion of network granulation into distinct subsections.
  - Briefly explain network granulation before introducing it as an attack strategy.

- **Highlight Qeios Focus:**
  - Briefly mention how this analysis of attack optimization contributes to the overall understanding of network vulnerability and resilience (e.g., informing defensive measures).

a. **Here's an example of a revised section incorporating these suggestions:**

4. Optimizing Network Vulnerability Analysis with Flow-Based Cores

This section explores how the flow-based approach can be used to optimize the analysis of network vulnerabilities.

A critical aspect of network vulnerability analysis is identifying the most impactful attack targets while minimizing the resources required for disruption. Here, we introduce the concept of flow-based cores (λ-cores). These cores represent functionally important subsystems within a network, identified based on information flow patterns.

The section demonstrates that λ-cores offer significant advantages over traditional structural k-cores in attack scenario building. By focusing on flow dynamics, λ-cores can pinpoint a smaller number of critical attack targets while achieving a similar level of disruption compared to k-cores. This is illustrated with the example of a hypothetical network where λ-cores require targeting a smaller number of nodes for network breakdown compared to k-cores.

Beyond node removal, the section also introduces the concept of network granulation. This strategy involves strategically disabling edges within the network to disrupt information flow. While not extensively explored in traditional network vulnerability analysis, network granulation offers a potential avenue for optimizing attack scenarios, especially when considering active defense measures.

Overall, the flow-based approach, through λ-cores and the consideration of network granulation, provides a more nuanced understanding of network vulnerabilities. This knowledge can be leveraged not only for offensive purposes but also to inform defensive strategies and enhance network resilience.

l. **Analysis of Conclusion**

This conclusion effectively summarizes the importance of network vulnerability analysis in the face of global challenges. Here's a breakdown of its strengths and areas for improvement:

a. **Strengths:**

- Emphasizes the growing need for network vulnerability analysis due to recent global challenges.
- Highlights the importance of understanding both structural and functional importance for effective protection.
- Concludes by reiterating the advantages of the flow-based approach for vulnerability analysis.

a. **Areas for Improvement:**

- **Focus and Neutrality:**
  - Tone down the language about "blocking" or prioritizing protection for offensive purposes.
  - Focus on the broader applicability of network vulnerability analysis for enhancing system resilience.
- **Clarity and Conciseness:**
  - Briefly summarize the key findings of the paper without excessive detail.
  - Consider restructuring or merging sentences for improved readability.

a. **Here's an example of a revised conclusion incorporating these suggestions:**

5. Conclusion

Recent events, including the COVID-19 pandemic and geopolitical conflicts, underscore the critical need for robust network vulnerability analysis. Understanding the vulnerabilities of complex systems, both structural and functional, is essential for developing effective protection strategies.

This paper presented a comparative analysis of structural and flow-based approaches to network vulnerability analysis. We explored methods for identifying critical elements within a network and demonstrated the advantages of the flow-based approach in capturing the cascading effects of disruptions.

By providing a more nuanced picture of network vulnerabilities, the flow-based approach can contribute significantly to improving system resilience across various domains. This knowledge can inform strategies for mitigating the impact of diverse threats, ultimately leading to more robust and adaptable systems.

This revised conclusion maintains the core message while removing potentially offensive language and emphasizing the broader applications of network vulnerability analysis beyond targeted attacks. It also streamlines the content and improves readability.

l. **Analysis of Bibliography**

The bibliography provides a comprehensive list of references relevant to network vulnerability analysis and complex systems. Here's a breakdown of its strengths and areas for improvement:

a. **Strengths:**

- Covers a wide range of sources, including scientific journals, conference proceedings, and reputable online sources.
- Includes recent publications (2020-2024) demonstrating the focus on current research.
- References on centrality measures, network cores, and flow analysis (items 15, 16, 21, 22, 23) directly support the content of the paper.

a. **Areas for Improvement:**

- **Formatting:**
  - Ensure consistent formatting for all references, especially online sources (items 11, 27, 28). Match the formatting style guide used in your paper.

a. **Here's an example of a revised reference for an online source:**

- **Original:** 11. ^https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote /index.html
- **Revised:** 11. North Atlantic Treaty Organization. (2021, November 30). Hybrid warfare: New threats, complexity and trust as the antidote. NATO Review

a. **Additional Notes:**

- Consider removing references that are not directly cited within the paper.
- If the paper is intended for a broader audience, some references to highly technical sources (e.g., item 17) might be replaced with more accessible options.

Specific examples of how the flow-based approach better captures cascading effects compared to the structural approach?

1. Epidemic Spread:

Consider a network representing a population where individuals are nodes and connections represent possible interactions. The spread of an infectious disease can be modeled as a flow through this network. Structural approaches, such as identifying highly connected nodes (super-spreaders) based on degree centrality, might miss the impact of nodes that are not as well-connected but play a crucial role in transmitting the disease between different clusters of the population.

The flow-based approach, on the other hand, considers the actual flow of the disease through the network, capturing the cascading effect of infections spreading from one node to another, even if those nodes are not directly connected. This allows for a more accurate identification of critical nodes that can significantly disrupt the disease spread.

2. Cascading Failures in Power Grids:

In a power grid, the flow of electricity can be modeled as a flow through a network of nodes (power stations, substations) and edges (transmission lines). Structural approaches to identifying critical nodes in power grids might focus on nodes with high degree or betweenness centrality. However, these measures might not fully capture the cascading effects of failures.

The flow-based approach, by considering the actual flow of electricity, can better capture the cascading impact of failures. For instance, a node with a relatively low degree but strategically positioned in the network could lead to widespread blackouts if it fails, disrupting the flow of electricity to downstream nodes.

3. Information Diffusion in Social Networks:

In social networks, the flow of information, such as news or rumors, can be modeled as a flow through a network of individuals (nodes) connected by social ties (edges). Structural approaches to identifying influential individuals might focus on nodes with high degree or closeness centrality. However, these measures might not fully capture the dynamics of information diffusion.

The flow-based approach, by considering the actual flow of information, can better capture the cascading effect of information spreading through the network. For example, an individual with a relatively small number of connections but positioned between different groups or communities could be highly influential in spreading information across the network.

In summary, the flow-based approach offers a more nuanced and dynamic understanding of network vulnerabilities by capturing the cascading effects of disruptions and identifying critical elements that might not be apparent through structural measures alone. This ability to better capture cascading effects makes the flow-based approach a valuable tool for analyzing and mitigating risks in various complex systems.

Additional interdisciplinary implications or applications of the flow-based approach that the authors might explore?

1. Transportation Networks and Traffic Congestion:

The flow-based approach can be applied to transportation networks to analyze traffic flow patterns and identify potential congestion hotspots. By considering the actual movement of vehicles and pedestrians through the network, the flow-based approach can provide insights into the dynamics of traffic congestion and inform strategies for improving traffic flow and reducing congestion.

2. Supply Chain Management and Disruption Mitigation:

In supply chains, the flow of goods and materials can be modeled as a flow through a network of suppliers, manufacturers, distributors, and retailers. The flow-based approach can be used to assess the vulnerability of supply chains to disruptions, such as natural disasters, political instability, or transportation bottlenecks. By identifying critical nodes and edges in the supply chain network, the flow-based approach can inform strategies for mitigating the impact of disruptions

and ensuring supply chain resilience.

3. Communication Networks and Information Security:

Communication networks, such as the Internet, can be modeled as a flow of information packets through a network of routers and switches. The flow-based approach can be used to analyze the security of communication networks and identify potential attack vectors. By considering the actual flow of information through the network, the flow-based approach can help identify critical nodes and edges that could be targeted by cyberattacks and inform strategies for network defense and security hardening.

4. Financial Systems and Systemic Risk:

Financial systems can be modeled as a flow of money and assets through a network of banks, financial institutions, and investors. The flow-based approach can be used to assess the systemic risk of financial systems and identify potential contagion effects. By considering the interconnectedness of financial institutions and the flow of funds through the system, the flow-based approach can inform strategies for mitigating systemic risk and preventing financial crises.

5. Public Health and Disease Surveillance:

Public health systems can utilize the flow-based approach to monitor the spread of infectious diseases and identify potential outbreaks. By considering the movement of individuals and the transmission of diseases through social networks, the flow-based approach can inform targeted interventions and resource allocation for disease control and prevention.

These examples demonstrate the broad applicability of the flow-based approach beyond network vulnerability analysis. By capturing the dynamics of flows and interactions within complex systems, the flow-based approach has the potential to provide valuable insights and inform effective decision-making in various interdisciplinary domains.