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

Ahmadreza Montazerolghaem[1]

1 Isfahan University

Potential competing interests: No potential competing interests to declare.

Overview

The article titled "Protection of Complex Network Systems from Targeted Attacks and Non-Target Lesions" by Olexandr Polishchuk delves into the vulnerabilities of complex network systems (NS) against various forms of attacks. The study presents a comparative analysis of structural and flow-based approaches to assess the impact and develop protection strategies against both targeted attacks and non-target lesions. The primary focus is on the importance of using a flow-based model to obtain a realistic understanding of the consequences of such attacks, highlighting the limitations of traditional structural models.

Key Contributions

1. **Comparative Analysis**:
    - The article provides a thorough comparison between structural and flow-based approaches for analyzing the vulnerability of network systems. It highlights that flow-based models offer a more realistic representation of attack consequences.
2. **Scenarios of Targeted Attacks**:
    - Different scenarios for targeted attacks are proposed, including successive targeted attacks on the most critical elements and simultaneous group attacks. These scenarios are evaluated based on both structural and flow models.
3. **Realistic Lesion Consequences**:
    - The study demonstrates that flow-based approaches provide a more comprehensive picture of the lesion's impact, capturing both direct and consequential damages more accurately than structural models.
4. **Optimizing Attack Scenarios**:
    - The paper introduces the concept of k-core and flow-core to optimize targeted attack scenarios, showing that targeting functionally important network components can achieve greater damage with fewer resources.

Detailed Sections

1. **Introduction**:
    - The introduction contextualizes the study within recent global challenges like the Covid-19 pandemic and the Russian-Ukrainian war, illustrating the relevance of studying network vulnerabilities. It sets the stage for discussing the impact of targeted attacks and non-target lesions on complex networks.
2. **Attacks on Network Structures**:
    - This section explains the mathematical foundation of complex networks, describing the adjacency matrix and centrality measures. It discusses various structural attack strategies and their implications on network integrity.
3. **Attacks on Network Operations**:
    - The article shifts focus to the operational aspect, emphasizing the flow model. It introduces the flow adjacency matrix and explains how analyzing flow disruptions provides a better understanding of attack impacts on network functionality.
4. **Optimization of Attack Scenarios**:
    - The optimization section presents methods to enhance attack strategies using structural and flow-based cores. It provides examples, such as the railway transport system of Western Ukraine, to illustrate the effectiveness of these methods.
5. **Conclusions**:
    - The conclusion summarizes the key findings and reinforces the superiority of flow-based models in understanding and mitigating the impacts of network attacks. It also underscores the need for continued research in optimizing protection strategies for complex networks.

Strengths

1. **Comprehensive Comparative Analysis**:
    - The paper effectively compares structural and flow-based models, providing a clear understanding of their respective strengths and limitations.
2. **Practical Relevance**:
    - By contextualizing the study with recent global events, the article highlights the practical significance of its findings and their applicability to real-world scenarios.
3. **Innovative Optimization Methods**:
    - The introduction of k-core and flow-core concepts for optimizing attack scenarios is a novel contribution,

demonstrating practical utility in minimizing resources while maximizing impact.

Weaknesses

1. **Limited Real-World Data**:
    - The study relies heavily on theoretical models and simulations. Incorporating more empirical data from real-world network systems would strengthen the findings and enhance their applicability.
2. **Complexity of Flow Models**:
    - While flow-based models provide detailed insights, their complexity might pose challenges in practical implementation, especially in large-scale networks.
3. **Focus on Destructive Strategies**:
    - The article primarily focuses on attack strategies. More emphasis on protective and preventive measures could provide a balanced perspective and enhance the practical utility of the research.

Suggestions for Improvement

1. **Incorporate Empirical Data**:
    - Integrating empirical data from actual network disruptions and attacks would validate the theoretical models and enhance the credibility of the findings.
2. **Simplify Flow Model Implementation**:
    - Developing simplified versions or guidelines for implementing flow models in real-world scenarios could make them more accessible to practitioners.
3. **Expand on Protective Measures**:
    - Including a more detailed discussion on protective strategies and countermeasures would provide a comprehensive approach to network security, balancing the focus between attack and defense.

Conclusion

The article presents a significant advancement in the study of network vulnerabilities, highlighting the superiority of flow-based models in understanding and mitigating the impacts of targeted attacks and non-target lesions. With further empirical validation and a balanced focus on protective measures, the findings could substantially enhance the security and resilience of complex network systems.