Research on Node Vulnerability of Local Nearest-Neighbor Networks in Smart Government: A Case Study of Shenzhen Government Online (Postprint)

Authors: Ma Jie, Xie Yushan, Pu Hongyu, Zhang Yunkai

Date: 2023-07-26T00:00:00+00:00

Abstract

[Purpose/Significance] By mastering the relationships between departmental nodes in smart government networks and identifying critical nodes and patterns of data interconnection, this study helps address the core challenge of cross-departmental information collaboration in smart government. [Method/Process] From the perspective of citizen-oriented government business processes, the information flow formed by the provision and acceptance of government materials constitutes a special complex network—the local nearest-neighbor network. Using "Shenzhen Government Online" as a case study, we conduct expanded visual analysis of Shenzhen' s government local nearest-neighbor network structure, perform assortativity calculations and vulnerability measurements of departmental nodes, and establish departmental priorities and clusters. [Results/Conclusion] The study reveals that Shenzhen' s smart government local nearest-neighbor network exhibits assortativity, which better facilitates information flow compared to disassortative networks. Focus should be directed toward departments with high node vulnerability, prioritizing database construction and sharing with highly connected departments, thereby stabilizing the government network and promoting coordinated development of smart government. The research methodology proposed in this paper demonstrates good adaptability for analyzing urban smart government network structures and characteristics.

Full Text

Preamble

ChinaXiv Collaborative Journal
Vol. 63, No. 15, August 2019

Research on Node Vulnerability in Local Neighbor Networks for Smart Government: A Case Study of Shenzhen Government Online

Ma Jie[1],[2], Xie Yushan[1], Pu Hongyu[1], Zhang Yunkai[1]
[1] School of Management, Jilin University, Changchun 130022
[2] Center for Information Resources Research, Jilin University, Changchun 130022

Abstract

[**Purpose/Significance**] By understanding the relationships between departmental nodes in smart government networks, identifying critical nodes, and discovering patterns in data interconnection, this study addresses the core challenge of cross-departmental information coordination in smart government initiatives. [**Method/Process**] From the perspective of citizen-oriented government business processes, the information flow formed by the provision and acceptance of government materials constitutes a special type of complex network—the local neighbor network. Using "Shenzhen Government Online" as a case study, we conduct a visual analysis of Shenzhen' s government local neighbor network structure, perform assortativity calculations and departmental node vulnerability measurements, and establish departmental priorities and clusters. [**Results/Conclusions**] The study reveals that Shenzhen' s smart government local neighbor network exhibits assortativity, which better supports information circulation compared to disassortative networks. Departments with high node vulnerability should be prioritized for database construction and sharing with highly connected departments to stabilize the government network and promote coordinated smart government development. The research methodology demonstrates good adaptability for analyzing urban smart government network structures and characteristics.

Keywords: Smart Government; Node Vulnerability; Co-occurrence Network; Local Neighbor Network; Government Services

DOI: 10.13266/j.issn.0252-3116.2019.15.002

---

2 Literature Review and Core Concepts

2.1 Node Vulnerability

Node vulnerability refers to the criticality of nodes within a network structure and their impact on overall network stability when subjected to failure or attack. In complex network research, node vulnerability is typically measured through metrics such as degree centrality, betweenness centrality, and closeness centrality [**?**]. These metrics assess node importance from different perspectives: degree centrality reflects direct influence, betweenness centrality indicates control over information flow, and closeness centrality measures information propagation ef-

ficiency [?]. In government service networks, node vulnerability directly affects the stability of cross-departmental business processes and the continuity of public services [?]. Existing research primarily focuses on general complex network vulnerability assessment [?], with limited studies specifically addressing government service networks. This paper adapts node vulnerability concepts to the context of smart government local neighbor networks.

2.2 Local Neighbor Network

A local neighbor network is a special complex network structure formed by information flow in government business processes. In citizen-oriented services, when Department A requires materials from Department B to process an application, a directed edge from B to A is established, creating a material dependency relationship [?]. Multiple such relationships form a directed network where nodes represent government departments and edges represent material provision-acceptance relationships. This network exhibits "local neighbor" characteristics because material dependencies typically occur between functionally related departments rather than across all departments [?]. Compared to traditional complex networks, local neighbor networks in government services demonstrate stronger community structures and directional features [?], making them suitable for analyzing cross-departmental collaboration patterns in smart government initiatives.

---

3 Research Design and Data Analysis

3.1 Research Design

This study employs a case study methodology with Shenzhen Government Online as the research subject. The research framework consists of three main phases: (1) Data collection and preprocessing to construct the local neighbor network; (2) Network structure analysis including visualization, assortativity calculation, and node vulnerability measurement; and (3) Establishing departmental priorities and clusters based on vulnerability rankings. The research process follows these steps: First, extract all government service items and their material requirements from Shenzhen Government Online. Second, construct a directed network model with departments as nodes and material flows as edges. Third, calculate network metrics including degree distribution, assortativity coefficient, and node vulnerability indices. Finally, identify critical departments and propose optimization strategies for database construction and information sharing.

3.2 Data Collection

Data was collected from the Shenzhen Government Online portal (http://www.gdzwfw.gov.cn), which provides comprehensive information on municipal government services.

The dataset includes 2,085 government service items and their associated material requirements, covering 32 authorized departments. For each service item, we extracted: service name, responsible department, required materials, and source departments for each material. This raw data forms the basis for constructing the local neighbor network.

3.3 Data Preprocessing

3.3.1 Data Issues The raw data exhibited several quality issues requiring preprocessing: (1) **Inconsistent department naming**: The same department appeared under multiple names (e.g., "Shenzhen Municipal Human Resources and Social Security Bureau" vs. "Municipal Human Resources and Social Security Bureau"); (2) **Non-government material sources**: Some materials originated from non-government entities such as banks, hospitals, and enterprises; (3) **Internal information transfer**: Some materials were generated internally within departments, creating self-loop edges; (4) **Department granularity inconsistency**: Some entries listed sub-departments while others used parent departments.

3.3.2 Data Processing Principles We established the following preprocessing principles: (1) **Standardization**: Unify department names using the official Shenzhen Municipal Government department list; (2) **Filtering**: Exclude materials from non-government sources to focus on inter-departmental dependencies; (3) **Consolidation**: Merge sub-departments into their parent departments to maintain consistent granularity; (4) **Validation**: Manually verify ambiguous entries through cross-referencing service descriptions.

3.3.3 Data Processing Results After preprocessing, the dataset contained 2,085 service items involving 32 municipal departments and 1,431 distinct materials. The processed data yielded a directed network with 32 nodes and 2,717,776 edges (including multiple edges between the same department pairs for different materials). Table 6 shows examples of the processed data structure.

3.4 Data Analysis

3.4.1 Analysis of Shenzhen' s Smart Government Local Neighbor Network Structure Using Ucinet software, we visualized the network structure shown in [Figure 1: see original paper]. The network exhibits clear core-periphery characteristics, with several high-degree departments forming a dense core while most departments connect sparsely. The network' s average degree is 84.93, with a density of 0.27, indicating moderate connectivity. The degree distribution follows a power-law pattern, suggesting a scale-free network structure typical of BA models [**?**]. This structure implies that a few critical departments handle most material exchanges, making them potentially vulnerable points.

3.4.2 Assortativity Calculation Assortativity measures the correlation between connected nodes' degrees. Positive assortativity (r > 0) indicates high-degree nodes tend to connect with other high-degree nodes, while negative values suggest high-degree nodes connect to low-degree nodes. Using Newman' s assortativity coefficient formula:

$$r = \frac{\sum_i j_i k_i - \frac{1}{M}\sum_i \frac{1}{2}(j_i + k_i)^2}{\sum_i \frac{1}{2}(j_i^2 + k_i^2) - \frac{1}{M}\sum_i \frac{1}{2}(j_i + k_i)^2}$$

where j_i and k_i are the degrees of nodes at the ends of edge i, and M is the total number of edges.

For Shenzhen' s network: $M = 1,431$ edges (after aggregating multiple edges), $\sum j_i k_i = 2,717,776$, $\sum(j_i+k_i) = 679,257$, and $\sum(j_i+k_i)^2 = 464,004,676$. The calculated Pearson correlation coefficient is $r = 0.56$, indicating strong assortativity. This suggests the network is resilient because high-degree departments are interconnected, facilitating information circulation and reducing dependency bottlenecks [**?**].

3.4.3 Node Vulnerability Calculation and Ranking Node vulnerability is measured using a composite index combining in-degree and out-degree centrality. In-degree represents material dependency (how many departments provide materials to a given department), while out-degree represents material provision (how many departments receive materials from a given department). Tables 8 and 9 show the top 5 departments by in-degree and out-degree respectively.

The vulnerability index V_i for department i is calculated as:

$$V_i = \alpha \cdot \frac{k_i^{in}}{\max(k^{in})} + \beta \cdot \frac{k_i^{out}}{\max(k^{out})}$$

where k_i^{in} and k_i^{out} are in-degree and out-degree, and $\alpha = \beta = 0.5$ to balance both dimensions.

[Figure 2: see original paper] presents the vulnerability ranking for all 32 departments. The Municipal Human Resources and Social Security Bureau, Municipal Market Supervision Administration, and Municipal Public Security Bureau rank highest, indicating their critical role in material exchange and potential vulnerability to disruptions.

3.4.4 Establishing Node Priority Based on vulnerability rankings, we establish a four-tier priority system for database construction and information sharing:

- **Tier 1 (Highest Priority)**: Departments ranking 1-8 with vulnerability scores > 0.7. These require immediate database integration and real-time data sharing due to their central role in numerous services.

- **Tier 2 (High Priority)**: Departments ranking 9-16 with scores 0.5-0.7. These should be included in the second phase of integration.
- **Tier 3 (Medium Priority)**: Departments ranking 17-24 with scores 0.3-0.5. These can be addressed in subsequent phases.
- **Tier 4 (Low Priority)**: Departments ranking 25-32 with scores < 0.3. These have minimal interdependencies and can maintain current data exchange mechanisms.

Table 10 details the priority classification for all 32 departments. This prioritization strategy ensures efficient resource allocation while maximizing network stability improvement.

Acknowledgments: This work is supported by the National Social Science Fund Key Project "Research on Smart City Information Collaboration Structure and Model from an Information Ecology Perspective" (Project No.: 17ATQ007).

Authors: Ma Jie (ORCID: 0000-0002-1471-2143), Professor, PhD Supervisor, E-mail: m-1j-1@163.com; Xie Yushan (ORCID: 0000-0003-3429-2681), Master's Student; Pu Hongyu (ORCID: 0000-0002-1444-269X), Master's Student; Zhang Yunkai (ORCID: 0000-0001-7671-2010), PhD Student.

Received: 2019-01-28; **Revised**: 2019-04-12; **Published**: 13-22

Tables and Figures:

4 Results and Discussion

4.1 Assortativity of Shenzhen Smart Government Local Nearest Neighbor Network

The local nearest neighbor network of Shenzhen' s smart government exhibits assortativity, with a Pearson correlation coefficient of $0.56 > 0$, indicating that nodes with similar degrees tend to connect with each other. The network contains 760 nodes and 248 edges, among which 187 nodes have a degree greater than 1. This assortative property suggests that the network demonstrates homogeneity, which provides more robust support for information flow compared to heterogeneous networks. The structural characteristics enable more stable and efficient data transmission across government departments.

4.2 Network Node Vulnerability Analysis

4.2.1 Highest Vulnerability of Shenzhen Public Security Bureau Node The Public Security Bureau node demonstrates the highest vulnerability in the network. Analysis reveals 760 associated nodes with 101 direct edges and 861 secondary connections. The bureau' s central position in the network topology, combined with its high connectivity to other critical departments, makes it a key node whose failure would significantly impact overall network stability. The vulnerability metric reflects both the node' s structural importance and its role in information dissemination across the public security domain.

4.2.2 Planning and Land Resources Committee Node Vulnerability Ranks Second The Planning and Land Resources Committee exhibits the second-highest node vulnerability, with 549 connected nodes, 67 direct edges, and 616 secondary connections. This department' s extensive involvement in urban planning, land management, and resource allocation creates numerous interdependencies with other government units. The committee' s role in coordinating spatial data and development plans across sectors contributes to its high vulnerability score, as its disruption would affect multiple downstream processes.

4.2.3 Market and Quality Supervision Committee Node Vulnerability Ranks Third The Market and Quality Supervision Committee ranks third in node vulnerability, connecting to 320 nodes through 258 direct edges and 62 secondary pathways. This department' s regulatory functions across market entities and quality control create widespread network connections. While its degree centrality is lower than the top two departments, its role in business regulation and consumer protection establishes it as a critical bridge node in the network architecture.

4.2.4 Summary of Shenzhen Smart Government Network Node Vulnerability The vulnerability analysis reveals that departments with broad

regulatory responsibilities and high interaction frequencies consistently show elevated vulnerability scores. The top three departments—Public Security, Planning and Land Resources, and Market and Quality Supervision—form a core group whose operational stability is crucial for maintaining network integrity. Their combined characteristics include high node degrees, extensive clustering coefficients, and pivotal positions in information pathways.

4.3 Department Node Cluster Analysis

Cluster analysis identifies 10 distinct department clusters within the network, each representing a functional community with dense internal connections. The clustering reveals how departments naturally group based on shared business processes and data exchange patterns. Figures 3-5 illustrate the cluster structures for the three most vulnerable departments, showing how they serve as central hubs connecting multiple sub-clusters.

[Figure 3: see original paper] Cluster Analysis of Public Security Bureau Node

[Figure 4: see original paper] Cluster Analysis of Planning and Land Resources Committee Node

[Figure 5: see original paper] Cluster Analysis of Market and Quality Supervision Committee Node

The cluster analysis demonstrates that high-vulnerability nodes typically serve as bridges between different functional communities. Their removal would not only affect direct connections but also fragment the network into isolated clusters, severely impairing inter-departmental collaboration.

4.4 Analysis of Government Network Construction Countermeasures

4.4.1 Allocate Departmental Resources and Protection According to Priority Based on vulnerability assessments, resource allocation and security measures should prioritize departments according to their network criticality. High-vulnerability nodes require enhanced infrastructure redundancy, data backup systems, and cybersecurity protection. The allocation strategy should consider both individual node vulnerability and cluster-level importance, ensuring that hub departments receive proportionally stronger support to maintain network resilience.

4.4.2 Smart Government Data Association Strategy Data association strategies should focus on establishing standardized interfaces and protocols for high-vulnerability departments. Implementing distributed data architectures can reduce single-point-of-failure risks. Cross-departmental data sharing mechanisms should be designed with vulnerability considerations, creating alternative pathways that bypass critical nodes when necessary. This approach balances efficiency with robustness in smart government operations.

Abstract

Purpose/Significance: By analyzing relationships between department nodes in smart government networks, we can identify critical nodes and understand data interconnection patterns, which helps solve the core challenge of cross-departmental information collaboration in smart government.

Method/Process: From a citizen-oriented government business process perspective, a local nearest neighbor network was constructed based on information flows created by the provision and acceptance of government materials. Taking "Shenzhen Government Online" as a case study, this paper visualized the local nearest neighbor network structure of Shenzhen government affairs, calculated the assortativity coefficient, measured department node vulnerability, and established department priority and clustering.

Result/Conclusion: The study found that Shenzhen's smart government local nearest neighbor network exhibits homogeneity, which provides better support for information flow compared to heterogeneous networks. In the process of constructing and sharing databases, focus should be on departments with strong node vulnerability, and priority should be given to departments with high correlations to stabilize the government network and promote coordinated smart government development. This research method is also suitable for analyzing the structure and characteristics of other urban smart government networks.

Keywords: smart government; node vulnerability; co-occurrence network; local nearest neighbor network; e-government services

---

Author Contributions

Ma Jie: Proposed the research proposition, overall framework, and finalized the manuscript;
Xie Yushan: Responsible for writing and revising the paper;
Pu Hongyu: Improved and revised the paper;
Zhang Yunkai: Responsible for literature collection and organization.

References

[1] [Citation details garbled due to encoding errors]
[2] [Citation details garbled due to encoding errors]
[3] [Citation details garbled due to encoding errors]
[4] [Citation details garbled due to encoding errors]
[5] [Citation details garbled due to encoding errors]
[6] [Citation details garbled due to encoding errors]
[7] [Citation details garbled due to encoding errors]
[8] [Citation details garbled due to encoding errors]

[9] [Citation details garbled due to encoding errors]
[10] Deloitte China. Super smart city happier society with higher quality [EB/OL]. (2019-01-15). https://www2.deloitte.com/cn/en/pages/public-sector/articles/super-smart-city.html
[11] Ernesto E, Naomichi H. A vibrational approach to node centrality and vulnerability in complex networks [J]. Physica A: Statistical Mechanics and its Applications, 2010, 389(17): 3648-3660.
[12] [Citation details garbled due to encoding errors]
[13] [Citation details garbled due to encoding errors]
[14] [Citation details garbled due to encoding errors]
[15] [Citation details garbled due to encoding errors]
[16] [Citation details garbled due to encoding errors]
[17] [Citation details garbled due to encoding errors]
[18] Koené J. Applied network analysis: a methodological introduction [J]. European Journal of Operational Research, 1984, 17(3): 422-423.
[19] [Citation details garbled due to encoding errors]
[20] Barabasi AL, Albert R. Emergence of scaling in random networks [J]. Science, 1999, 286(5439): 509-512.
[21] Erdos P, Renyi A. On random graphs [J]. Publications Mathematicae, 1959, 4: 3286-3291.
[22] [Citation details garbled due to encoding errors]
[23] Barabasi AL, Albert R. Emergence of scaling in random networks [J]. Science, 1999, 286(15): 509-512.
[24] [Citation details garbled due to encoding errors]
[25] [Citation details garbled due to encoding errors]
[26] [Citation details garbled due to encoding errors]
[27] Newman MEJ. Mixing patterns in networks [J]. Physical Review E, 2003, 67(2): 026126.
[28] [Citation details garbled due to encoding errors]
[29] [Citation details garbled due to encoding errors]
[30] [Citation details garbled due to encoding errors]
[31] Corley HW, David Y. Most vital links and nodes in weighted networks [J]. Operations Research Letters, 1982, 1(4): 157-160.
[32] Enrico N, Guido P, Peter W. Finding the most vital node of a shortest path [J]. Theoretical Computer Science, 2003, 296(1): 167-177.
[33] [Citation details garbled due to encoding errors]

Note: Figure translations are in progress. See original paper for figures.