machines

MDPI

Article

Cascading Failure Analysis of Hierarchical Industrial Wireless Sensor Networks under the Impact of Data Overload

Hongchi Lv [1,2], Zhengtian Wu [1,2,*], Xin Zhang [1,2,*], Baoping Jiang [1,2] and Qing Gao [3]

[1] School of Electronic and Information Engineering, Suzhou University of Science and Technology, Suzhou 215000, China; 2013041032@post.usts.edu.cn (H.L.); bpjiang@usts.edu.cn (B.J.)
[2] Suzhou Smart City Research Institute, Suzhou 215000, China
[3] School of Automation Science and Electrical Engineering, Beihang University, Beijing 100191, China; gaoqing@buaa.edu.cn
* Correspondence: wzht8@mail.usts.edu.cn (Z.W.); xwzj@usts.edu.cn (X.Z.)

Abstract: As industrialization accelerates, the industrial sensor network environment becomes more complex. Hierarchical multi-cluster wireless sensing network topology is generally used due to large-scale industrial environments, harsh environments, and data overload impact. In industrial wireless sensor networks, the overload of some nodes may lead to the failure of the whole network, which is called cascading failure. This phenomenon has incalculable impact on industrial production. However, cascading failure models have mainly been studied for planar structures, and there is no cascading failure model for hierarchical topologies in industrial environments. Therefore, this paper built a cascading failure model for hierarchical industrial wireless sensor networks (IWSNs) for realistic industrial network topologies. By establishing an evaluation mechanism considering the efficiency of the network and the viability of nodes, the network communication efficiency that is not considered in the traditional evaluation mechanism is solved. In addition, aiming at the problem of network topology changes caused by node failure, dynamic load distribution methods (ADD, SLD) are used to improve network invulnerability. Theoretical analysis and experimental results show that the traditional allocation method (SMLD) does not apply in hierarchical topologies; when the general cluster head node capacity is moderate, increasing the capacity of single-hop cluster head nodes can prevent cascading failures more effectively.

Keywords: hierarchical architecture; industrial wireless sensor networks; cascading failure; data overload

Citation: Lv, H.; Wu, Z.; Zhang, X.; Jiang, B.; Gao, Q. Cascading Failure Analysis of Hierarchical Industrial Wireless Sensor Networks under the Impact of Data Overload. *Machines* **2022**, *10*, 380. https://doi.org/10.3390/machines10050380

Academic Editor: Mosè Gallo

Received: 12 April 2022
Accepted: 13 May 2022
Published: 16 May 2022

1. Introduction

1.1. Motivation

Wireless sensors have played a crucial role in various intelligent devices in the past decades. They are an essential engine driving information technology transformation. These devices carry the function of autonomous data collection, intelligently communicate, process information with each other, and integrate and process the data for transmission to end devices. In IWSNs, the overload of some nodes may lead to the failure of the whole network; this phenomenon is called cascading failure [1]. When building a complex network, the interaction and dependence between devices make cascading failures a major threat. Especially in the industrial network environment, the node overload phenomenon caused by factors such as colossal network scale, heterogeneous system, and working environment is the bottleneck restricting the development of industrialization.

Although there have been promising results for WSNs, there is little research on the cascading failure of IWSNs. Compared with traditional WSNs, there are differences in the following aspects:

- Under the influence of harsh industrial environments (such as noise, exhaust gas, dust, and high temperature), industrial wireless sensors pose severe challenges to the survival and stability of the network, which becomes more prone to cascading failures;
- High topology complexity means that the network node layout in the industrial site is more complex, and the coverage is more considerable. Using the simple networking topology (e.g., star topology) is not suitable;
- The real-time performance of data transmission, in some scenarios, requires data to be transmitted at a breakneck speed to reduce the risk of accidents.

Due to the above differences, it is essential to explore the cascading failure phenomenon in the hierarchical topology of IWSNs. The robustness of the network should integrate the network-efficiency value and the node-survival number under cascading failures. This paper provides theoretical guidance for building industrial sensor networks, thereby reducing the probability of large-scale losses caused by cascading failures.

1.2. Literature Review

1.2.1. Research Status of IWSNs

The rapid development of industrial manufacturing has produced many meaningful process transformation schemes [2,3]. Meanwhile, there are also many valuable theories and methods for the research of IWSNs. Kumarage et al. [4], aiming at disseminating industrial wireless networks and the limitation of sensors themselves, proposed a robust and scalable mechanism to accurately and effectively detect negative anomalies. Raza et al. [5] detailed the design goals, challenges, and solutions of IWSNs, conducted a comprehensive review of existing standards and industry protocols, and critically assessed the potential of these standards and protocols. Available hardware platforms, specific industrial energy harvesting technologies, and capabilities are discussed in detail. Jan et al. [6] discussed the design challenges of cluster-based schemes, important cluster formation parameters, and classification of hierarchical clustering protocols. Furthermore, existing cluster-based and grid-based technologies are evaluated by considering specific parameters to help users choose an appropriate technology. In Rostami et al. [7], several clustering methods are studied to demonstrate their advantages and disadvantages.

In the field of IWSNs, distributed wireless sensors have been widely studied and have solved a large number of real-world problems. For example, [8] proposed the first distributed MAC protocol to minimize the access delay by optimizing the window size in the power competition. This method has better access delay and packet arrival rate by simulation. Furthermore, [9], aiming at the problem of signal mixing caused by a complex industrial environment, proposed a signal classification method based on feature signal fusion, which performs down-frequency and sampling preprocessing on the signal received by the node to obtain an intelligent representation of the movement. Borgiani et al. [10] proposed distributed congestion control by duty-cycle restriction to detect and mitigate DoS in the Industrial Internet of Things. The ability to reduce detection and mitigation times can be compared to centralized approaches. For the deployment problem of a 3D industrial space with obstacles, [11] proposed a distributed parallel particle swarm optimization to maximize the coverage and prolong the life cycle. Gholami et al. [12] reported and analyzed distributed systems for industrial sensor and control applications. They discussed two aspects: wireless sensor network localization and node self-organizing clustering.

Most of these distributed WSNs consider two aspects: (1) the optimization of network topology [11,12] and (2) the optimization of network routing protocols and algorithms [8–10]. However, the cascading failures caused by dependencies between network devices are ignored in these studies. The phenomenon of cascading failures is catastrophic, so from the perspective of complex networks, understanding the causes of cascading failures and modeling their behavior and effects is crucial and irreplaceable to ensure the reliable operation of network systems [1].

1.2.2. Research Status of Cascading Failure

Due to the advancement of informatization, the number of nodes in various networks has doubled. Network topology has become more complex, making cascading failures more common. Cascading failures are commonly found in sensor networks [13,14], transportation systems [15–17], and power systems [18,19]. In sensor networks research on cascading failure, Zhao et al. [20] studied the topological characteristics of WSNs based on complex network theory. The impact of different types of nodes on the invulnerability of sensor networks was analyzed from the perspective of the destructiveness of complex networks. Tan et al. [21] proposed a new energy-efficient and fault-tolerant evolution model for large-scale wireless sensor networks based on complex network theory. In the evolution model, not only the residual energy of each node is considered, but also the link constraints are introduced to make the energy consumption of the whole network more balanced. Liu et al. [22] established scale-free topology cascading failure networks. Then the cascading failure control method was proposed according to the critical load. Fu et al. [23] divided the network load of wireless sensors into two types: link-oriented and node-oriented. Through cascading failure simulation, it was found that the minimum cost required to defend against intentional node attacks is more expensive than that required to face intentional link attacks. The research direction from sensor network cascading failure, in turn, is based chiefly on peer-to-peer planar structures and coupled networks [24]. Due to the lack of research on cascading failures in hierarchical topology, this research is very meaningful.

Many research results have been obtained in the cascading failure model on overload research [25–27], evaluation mechanism [27–29], capacity definition [23], load redistribution [30,31], and critical assessment [28,32,33]. These research results provide theoretical support for building healthy networks. In [28], a reasonable global load redistribution model was designed for communication networks, and it was found that the centrality can accurately reflect cascading failures. Potts et al. [29] used two standard centrality metrics as a measure of network viability to assess the robustness of the network to vertex deletion, evaluated the advantages and disadvantages of network analysis techniques in assessing system architectures, and targeted guidelines for architecture robustness assessment. Zhong et al. [27] proposed a durability evaluation method based on the load-dependent overload model. It was found that network durability was strongly dependent on the initial disturbance strength and the cascading strength. Network durability with a uniform initial load distribution typically increases monotonically with decreasing initial disturbance strength. In contrast, durability behavior is more complex for other initial load distributions. Hou et al. [31] studied the heterogeneous load-redistribution mechanism in a simplified sand-pile model. We find that weak heterogeneity in load redistribution can effectively mitigate cascades, while substantial heterogeneity in load redistribution can even enlarge the size of the final failure. Liu et al. [34] introduced a self-healing model for overload propagation in complex networks caused by malicious attacks. We find that, during self-healing, the optimal recovery time for both the model and the real-world network exists within a given recovery resource. Shen et al. [35] proposed an interdependent network cascading fault model based on mutual traffic redistribution under load fluctuations. In the model, the traffic loss related to the existing resources of the network is considered by defining the traffic-loss parameter. The results show that larger node tolerance and more significant flow loss parameters can improve network robustness. In [36], a new definition of node load is proposed based on the load-capacity (LC) cascading fault model. Attenuation and exponential coefficients are added to the LC model to achieve a greater degree and more substantial load capacity.

1.3. Our Contribution

In order to study the overload cascading failure of industrial sensor networks with hierarchical topologies, the main contributions of this paper are as follows:

1. Different from previous cascading failure planar structural models, a parameter-adjustable cascading failure simulation model with hierarchical architecture is established to make its network topology closer to the actual scenario;
2. To address the problem that conventional destructibility metrics are not applicable to industrial complex environments, the destructibility measure is optimized by combining communication efficiency and direct connection survivability;
3. Aiming at the problem that the allocation strategy of the planar structure is not suitable for the hierarchical structure, we adopt the dynamic capacity allocation methods. Through experiments, the invulnerability of the network can be improved.
4. According to the characteristics of cascading failure hierarchical topology, we study the impact of single-hop cluster head node capacity on the network's re-resistance to damage, to provide a reference for building a higher quality network.

The rest of this paper is structured as follows. Section 2 describes the cascading mechanism, load-capacity model, and allocation mechanism of the industrial wireless sensor hierarchical topology. In Section 3, this paper's improvement and optimization scheme is proposed. In Section 4, the scheme's feasibility is verified by comparing simulation data. Finally, the conclusion is given.

2. Preliminaries

2.1. Hierarchical Topology of IWSNs

Industrial wireless sensor networks can be structurally divided into planar and hierarchical structures. In the planar structure, each sensor node has the same functional attributes. Flooding is used in data collection by the sink node to send query commands to all sensor nodes in the region [37]. Due to the universality of this structure, existing wireless sensor cascading failure models are mainly studied for planar structures. Table 1 shows some planar structural networks for cascading-failure studies. However, for more complex industrial wireless sensor-network environments, the hierarchical topology is more practical, because the cluster head nodes in the hierarchical structure can fuse the raw data and improve the efficiency of the network [38]. In this structure, the sensor network consists of multiple clusters, and the nodes are divided into cluster head nodes in the upper-level network and general nodes in the lower-level network. The role of the general nodes in the lower layer is to collect and detect the collected environmental data and then transmit the data to the cluster head node where they are located. The cluster head node aggregates and processes the data in this cluster and transmits the processed data to the sink node by multi-hop relaying. Figure 1 shows the hierarchical topology of industrial wireless sensor networks; this type of hierarchical topology approach dramatically improves the efficiency of information processing and transmission.

Table 1. Some planar structural networks for cascading failure studies.

Related Literature	Network Structure
[20,22,30]	scale-free network
[21,28]	Barabási–Albert (BA) network
[15,26,39]	reality network
[24,39,40]	coupled network

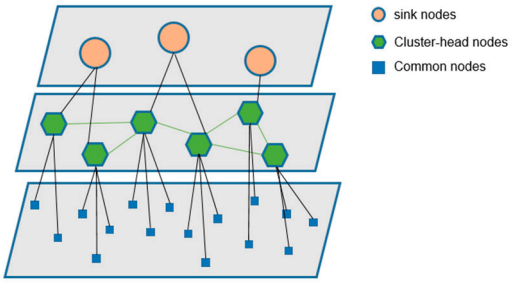


Figure 1. Hierarchical topology of industrial wireless sensor networks.

2.2. Cascading Failure Mechanism

In industrial field scenarios, wireless sensor networks are usually required to transmit complex data, including sound, images, film, and video, to meet each task scenario's needs, so wireless sensor nodes suffer from more significant data overload impact [23]. When damage to the node leads to a change in the network topology, it redistributes data traffic transmission. Subject to the hardware cost, there is no guarantee that the node processing capacity is always more significant than the load, thus causing a new round of traffic redistribution, which will eventually cause a large-scale cascading failure of the network.

Due to the hierarchical topology approach, common nodes only need to collect environmental data, the cluster head nodes integrate the data and transmit them to the sink nodes through multi-hop transmission, the sink nodes provide data to the terminal devices. The multi-hop transmission method between cluster head nodes makes cascading failures occur only between cluster head node layers [41]. As shown in Figure 2, cluster head node 1 is not working properly due to data shocks or external environmental damage, so the data originally forwarded and collected by node 1 needs to be transmitted to the adjacent nodes 2, 3, and 5. The adjacent nodes receive the load from node 1 according to a certain distribution ratio. Unfortunately, the current network load of nodes 3 and 5 exceeds their maximum processing range, causing node 3 and node 5 to fail. This action will eventually cause a large network crash.

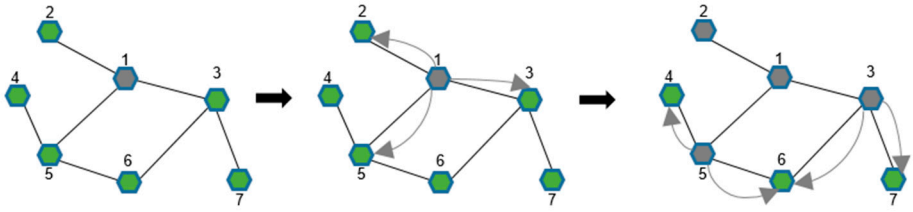


Figure 2. Cascading-failure process between cluster head nodes.

2.3. Load-Capacity and Allocation Mechanisms

Sensor load refers to the total amount of data traffic collected and forwarded by a node per unit time, and the capacity represents the upper limit of load that a node can bear [39]. Hierarchical industrial wireless sensors usually consist of cluster head nodes and general nodes. The general node is responsible for collecting information in the covered area and aggregating the data to the cluster head node. The cluster head node not only handles the information collection within the cluster but also undertakes the task of forwarding data from other cluster head nodes. For general nodes and sink nodes, the capacity is always guaranteed to be larger than the load at the beginning of building the network. However, cluster head nodes need to transmit data in real-time, so their load is updated at each time. Therefore, it is vital to quantify the cluster head node's load and capacity. There are two methods that are often used to define the load on cluster head nodes. The first method is measured in degrees [23,39]:

$$L_i(0) = k_i^{\sigma}, \tag{1}$$

where $L_i(0)$ is the initial load of the node i, σ is used to adjust the variability of the initial load, called the weight factor, and the number of edges connected to the specified node is used to describe the load of the initial node. However, this approach considers only the degree of the nodes. Some metrics describing the importance of the nodes are ignored.

The second method is to use betweenness [28] to measure the load of the nodes:

$$L_i(0) = (B_i / \frac{N(N-1)}{2})^{\sigma}, \tag{2}$$

where B_i is the betweenness of the node i. Although this takes into account some necessary information about the network topology, it is not suitable for large-scale network architectures, because this approach requires a lot of computation.

The capacity represents the upper limit of the load a node can carry. For cluster head nodes, the capacity is generally fixed and positively related to the initial load of the node [23,39].

$$C_i = (1 + \lambda)L_i(0), \tag{3}$$

where C_i represents the capacity of the node, and λ is the overload tolerance factor.

When the network suffers from overload impact resulting in the cascading phenomenon, a common method of allocation mechanism is based on the static metrics [17,25] (e.g., degrees, betweenness) of neighboring nodes. We call it static metrics load distribution (SMLD), which can be expressed as follows.

$$\eta_j = \frac{k_j}{\sum_{n \in \Gamma_i} k_n}, \tag{4}$$

where η_j denotes the load distribution rate from i to j; k_j is the degree of the node, and Γ_i collects the neighboring nodes.

3. Main Results

In this section, an improvement and optimization scheme is proposed. Firstly, to address the problem that conventional destructibility metrics do not applicable to complex industrial environments, this article combines communication efficiency and direct connection survivability to optimize the destructibility measures. Secondly, cascading failure occurs only between cluster head nodes, so this paper quantified the load on cluster head nodes. Finally, two dynamic allocation strategies are used to improve the network and address the shortcomings of existing allocation mechanisms.

3.1. The Improved Evaluation Mechanism of IWSNs

Invulnerability represents the network's survival after suffering cascading failure. The higher the invulnerability metric, the less impact the network will have after experiencing cascading failure. The commonly used evaluation method is gain components [26], which can be computed as follows:

$$G = \frac{N_r^f}{N_r}, \tag{5}$$

where G is the gain component; N_r represents the number of nodes, and N_r^f represents the normal nodes after cascading failure.

However, this evaluation mechanism is not applicable in large hierarchical industrial wireless sensor networks. The reason is that, although some nodes survived from the cascading failure, the links to the sink nodes have been severed. They are unable to communicate with the sink nodes. Such nodes should not be counted when evaluating the network. Moreover, even though the communication can still be connected, more relay nodes are required, which greatly affects the communication efficiency problem, and the

above evaluation metrics do not describe the communication efficiency. To solve the above problems, the following evaluation metrics are proposed.

$$E = \frac{\sum_{i \in r} \frac{1}{d_{ik}}}{N_r(N_r - 1)}, \tag{6}$$

where E is the efficiency measure, which is a metric to quantify the communication efficiency of nodes; d_{ik} denotes the shortest path length from relay node i to sink node k; N_r is the number of nodes;

$$M = \frac{N_r^{(k)} E(t)}{N_r E(0)}, \tag{7}$$

where M is the new proposed evaluation mechanism. $N_r^{(k)}$ is the number of remaining links between nodes and node k, which removes the surviving but isolated nodes. The ratio of the initial communication efficiency $E(0)$ to the current communication efficiency $E(t)$ shows the change in efficiency due to cascading failure. The new proposed evaluation mechanism both ensures the accuracy of the network's surviving nodes and quantifies the network's communication efficiency.

3.2. The Improved Load and Capacity Metrics of IWSNs

In the above two methods of expressing node loads, one considers only a single parameter, and the other considers global variables, for which the required computational effort is too considerable. To the practical situation of hierarchical sensor networks, the load of cluster head nodes is not only related to the number of connected lower layer general nodes but also closely related to the neighboring cluster head nodes on the same layer. Therefore, this paper defines the initial load of cluster head nodes as the product of node degree and related adjacent node degree. The initial load can be computed as follows:

$$L_i(0) = \left(\sum_{j \in \Gamma_i} \frac{k_j}{D_a} k_i\right)^{\sigma}, \tag{8}$$

where L_i is the load of i; k_i represents the degree of the node i; k_j is the degree of the node j; Γ_i collects the neighboring nodes of i, and D_a means the average degree of all networks. σ is used to adjust the variability of the initial load, called the weight factor. This method considers the local information of nodes, which can reflect the node load information more realistically in the case of less computation.

In this model, a linear relationship between the load L_i and the capacity C_i is used. By adding an exponential adjustment parameter to the original capacity-load model, the two parameters for adjusting capacity can be matched to provide more accurate capacity adjustment. It can be expressed as:

$$C_i = (1 + \lambda) L_i(0)^{\beta}, \tag{9}$$

where λ is the overload tolerance factor, and β is the exponential adjustment parameter. By adjusting the size of λ and β to expand the capacity of the nodes, in reality, the expansion of capacity will cost more, so infinite growth cannot be achieved. Meanwhile, in order to explore the impact of the capacity of single-hop cluster head nodes on the destructive capability of the network, the nodes directly connected to the sink node are defined as $\beta_{special}$.

3.3. The Improved Dynamic Allocation Method

When the static metric allocation method mentioned above is applied to a real large-scale hierarchical industrial wireless sensor networks, the capacity of neighboring nodes may be close to saturation and can not bear the excess load. If the load redistribution is forced according to the static initial metric allocation method of the nodes, it will undoubtedly lead to the failure of the neighboring nodes.

Furthermore, when a node determines that there is a load to be redistributed, the node with higher degree among the neighboring nodes has a higher probability to take on more load-distribution tasks. To solve this problem, two real-time dynamic allocation methods are used in this paper, the first one is the average degree distribution (ADD). For each time step t, the load is allocated in real time according to the residual load ratio ψ:

$$\psi_j(t) = \frac{C_j(t) - L_j(t)}{C_j(t)}, \tag{10}$$

The load distribution rates are as follows:

$$\eta_j(t) = \frac{\psi_j(t) C_j(t)}{\sum_{n \in \Gamma_i} \psi_n(t) C_n(t)}. \tag{11}$$

The second way is surplus load distribution (SLD). The load distribution ratio is as follows:

$$\eta_j(t) = \frac{k_j}{\sum_{n \in \Gamma_i} k_n(t)}, \tag{12}$$

where $k_n(t)$ represents the degree of the node n at time t. $k_n(t)$ dynamic real-time detection is required, rather than being decided at the initial network construction.

When the dynamic load distribution is complete, the current load of each node is as follows:

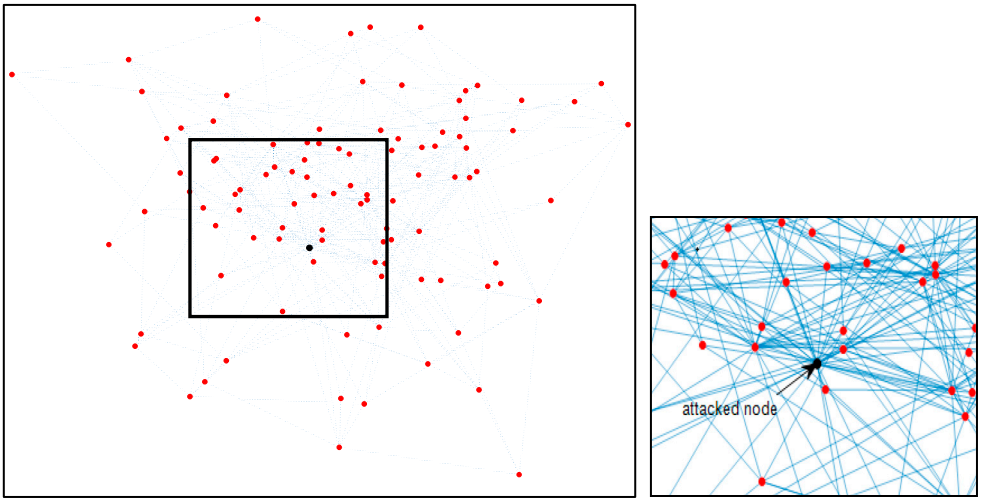
$$L_j(t) = L_j(t-1) + \eta_j(t) L_i(t-1), \tag{13}$$

when $L_j(t) > C_j$, the cascading failure process occurs until $L_j(t) \leq C_j$.

4. Simulations

This section verifies the scheme's feasibility by comparing simulation data. Firstly, evaluation mechanisms are compared to verify the rationality of the improvement. Secondly, this paper adjusted the size of node capacity to suppress the effect of cascading failure, which provides ideas for the rational matching of network node capacity. Finally, three dynamic redistribution strategies are compared.

In this paper, a hierarchical network with one sink node, 100 cluster head nodes, and 416 common nodes is simulated. Sensors have a limited ability to process information, and data that cannot be processed at this moment will always be present in every subsequent time unit. It is worth noting that the degree of a node in the paper contains the total number of connected paths of the general nodes in the lower level and the neighboring nodes in the same level. Since the probability of cascading failure is higher for nodes with a higher degree in hierarchical networks, this paper adopts a deliberate attack on the node with the highest degree in the network to simulate the natural phenomenon of cascading failure caused by a data-overload impact on nodes. The topology of the cluster head node layer is shown in Figure 3.



(**a**) (**b**)

Figure 3. The topology of the cluster head nodes: (**a**) the complete cluster head nodes topology and (**b**) the partially enlarged view of the attacked node.

4.1. Comparison of Evaluation Indicators

In this subsection, to compare the commonly used metrics for cascading failures in Equation (5) with the metrics proposed in Equation (7), we use Equation (8) to define the cluster head node load, letting $\sigma = 0.2$. The node capacity is adjusted by the exponential adjustment parameter in Equation (9), letting $\lambda = 0.8$. The communication efficiency of the overall network is calculated by Equation (6). The comprehensive evaluation indicators in Equations (5) and (7) are compared. By simulation, the results are as follows.

As shown in Table 2, the evaluation metrics M proposed in this paper are consistently lower than the commonly used G. This is a more realistic phenomenon in hierarchical industrial wireless sensor networks. For example, when $\beta = 0.3$, there are a total of 17 cluster head nodes surviving, yet only 13 cluster head nodes can connect to the sink node. Moreover, for the network efficiency, even though the number of survivors is similar, M and G differ significantly. This is because M takes into account the variation in transmission distance. Compared with the original network, the transmission distance is greatly increased and the network efficiency is greatly reduced, because the path to the convergence node is destroyed, and the original evaluation index does not reflect the network-efficiency problem. Therefore, the reasonableness of M can be verified.

Table 2. The experimental data.

Exponential Adjustment Parameter β	Number of Surviving Nodes		Communication Efficiency E ($\times 10^4$)	Comprehensive Evaluation Indicators	
	M	G		M	G
0.1	0	0	0	0	0
0.2	0	5	0	0	0.050
0.3	13	17	4.91	0.017	0.170
0.4	0	7	0	0	0.070
0.5	78	78	32.39	0.631	0.780
0.6	85	85	35.37	0.751	0.850
0.7	87	87	36.05	0.784	0.870
0.8	92	92	37.75	0.867	0.920
0.9	94	94	38.68	0.908	0.940
1.0	96	96	39.28	0.941	0.960
1.1	99	99	40.22	0.993	0.990

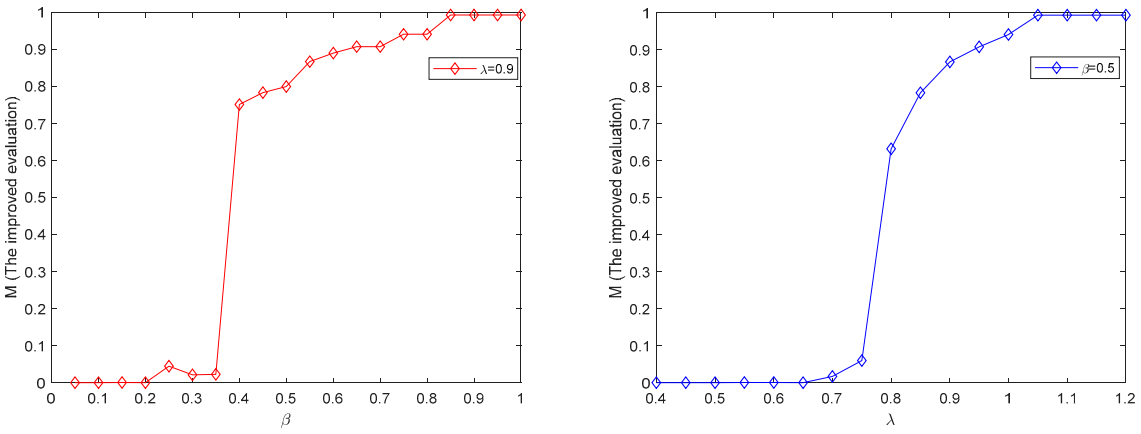
4.2. Impact of Some Parameters on the Invulnerability Performance

The magnitude of M and G reflects the invulnerability performance of the networks. When the value is 0, the network is totally collapsed, and when the value is 1, the network does not suffer from cascading failure. This paper adjusted the size of the node capacity to suppress the effect of cascading failure, which provides ideas for the rational matching of network node capacity.

4.2.1. Effect of Capacity Regulation Parameters

In Section 3.2, the overload tolerance factor λ and the exponential adjustment parameter β have an effect on the node capacity. To explore their respective effects on invulnerability performance, we let $\sigma = 2$ to conduct the experiment.

As shown in Figure 4, from (a), when $\lambda = 0.9$, M oscillates with the increase of β. When $\beta > 0.8$, M no longer increases. When $\beta = 0.8$, the efficiency of the network and the number of surviving nodes are optimized. The conclusion of (b) is similar to (a), except that M does not increase as fast as (a), which means that the network performance is more sensitive to β. Meanwhile, it is unreasonable to blindly increase the capacity factor of the network and increase the cost of network construction for nothing. This conclusion is consistent in planar coupled networks [40] and single-layer networks [26].



(**a**) (**b**)

Figure 4. Effect of capacity regulation parameters: (**a**) the effect of exponential adjustment parameter on invulnerability performance and (**b**) the effect of overload tolerance on invulnerability performance.

4.2.2. Impact of Single-Hop Cluster Head Node Capacity

In the experiment, we found that the damage of the network is related to the single-hop cluster head node to a certain extent. We divide the cluster head nodes into single-hop cluster head nodes and general cluster head nodes, and their capacity size is determined by Equation (9). Single-hop cluster head nodes, as nodes directly adjacent to the sink nodes, become the mandatory path to the sink nodes. Let $\sigma = 2$, $\lambda = 0.55$, and then we explored the impact of single-hop cluster head node capacity on the invulnerability of the whole network.

As shown in the Figure 5, the evaluation index is set to M. It is clear to see that increasing the capacity of single-hop cluster head nodes does not increase the number of available nodes in the whole network in the small case. In contrast, when the capacity of single-hop cluster head nodes is gradually increased, the propagation of cascading faults can be effectively suppressed. However, when the overall capacity of the network is large enough, expanding the capacity of single-hop nodes does not significantly improve the resilience of the network to damage; it only causes a waste of resources.

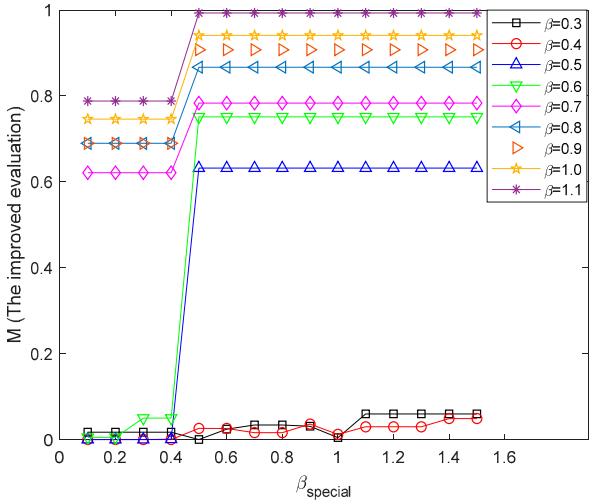


Figure 5. The influence of single-hop cluster head node capacity on G.

As shown in Figure 6, when the evaluation index is the original evaluation index G, the value of M is much smaller than the value of G when $\beta \in [0.3, 0.4]$. This is because, although the number of surviving nodes is large, the critical paths that can be transmitted to the sink node are destroyed, resulting in a substantial increase in the shortest paths of the surviving nodes. This can directly reflect the reasonableness of the improved evaluation index.

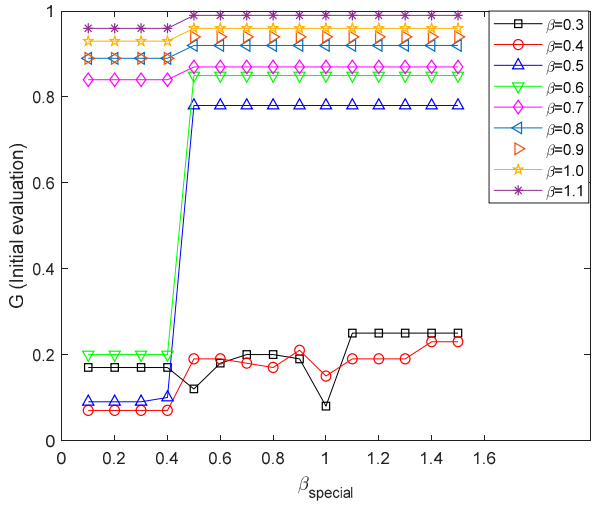


Figure 6. The influence of single-hop cluster head node capacity on M.

In reality, the increase of β means an increase in cost. Therefore, this experiment provides an important theoretical guidance for constructing an economical and more destructive network.

4.3. Impact of Dynamic Redistribution Strategies on Invulnerability Performance

This subsection focuses on the impact of redistribution strategies on network invulnerability. We simulated three load-redistribution strategies (SMLD, ADD, SLD) on cascading failures, and the load distribution rate is reflected in Equations (4), (11) and (12), respectively.

From the Figure 7, we can see that ADD and SLD are significantly better than SMLD, although SMLD is practical in other networks. The reason why SMLD performs poorly in this model is that this paper considers a hierarchical topology. Although the capacity is allocated according to the degree correlation, the cluster head node with a higher degree

may have a higher amount of out-of-layer degrees and a lower amount of intra-layer degrees, resulting in unreasonable capacity allocation and serious cascading failures.

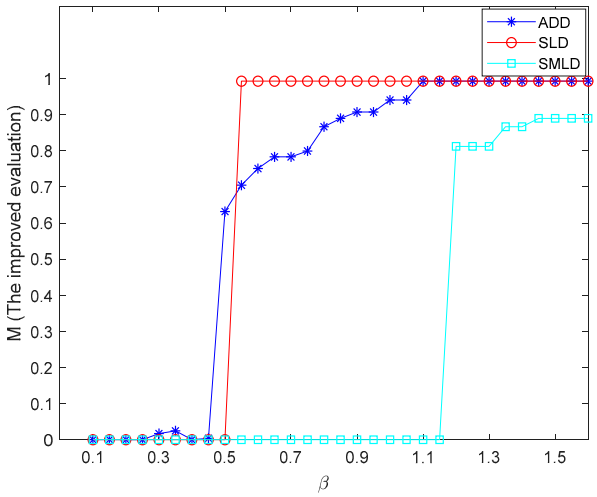


Figure 7. The influence of different distributions working on M.

We can also found that the network survival rate under ADD and SLD is significantly improved when $\lambda \in [0.45, 0.55]$, and ADD has better results in the early stage. However, compared to the threshold value for full network survival, the network can be fully survived under the SLD when $\lambda = 0.55$. In contrast, ADD can achieve the same effect when $\lambda = 1.1$.

5. Conclusions

This paper establishes a cascading-failure model of hierarchical industrial wireless sensor-networks topology to meet the needs of large industries. This model combines node survival rate and communication efficiency to improve the evaluation mechanism. The impact of single-hop node capacity expansion on network invulnerability is studied. We found that the effects of capacity regulation parameters on hierarchical networks are consistent with that of planar structure networks. Then, a comparison of the three distribution methods under dynamic topology is given through simulation. Theoretical analysis and experimental results show that the traditional allocation method (SMLD) does not apply in hierarchical topologies.

Author Contributions: Conceptualization, Z.W.; Funding acquisition, Z.W. and X.Z.; Methodology, X.Z.; Software, H.L.; Supervision, B.J.; Writing—original draft, H.L.; Writing—review and editing, X.Z. and Q.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research has been supported by the Natural Science Research of Jiangsu Higher Education Institutions of China under grant 21KJB120010 and the Natural Science Foundation of Suzhou University of Science and Technology under grant 342131604.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors are grateful to the anonymous reviewers and the Editor for their valuable comments and suggestions on improving this paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Xing, L. Cascading Failures in Internet of Things: Review and Perspectives on Reliability and Resilience. *IEEE Internet Things J.* **2020**, *8*, 44–64. [CrossRef]
2. Xiao, X.; Roh, B.-M.; Zhu, F. Strength Enhancement in Fused Filament Fabrication via the Isotropy Toolpath. *Appl. Sci.* **2021**, *11*, 6100. [CrossRef]
3. Xiao, X.; Joshi, S. Process planning for five-axis support free additive manufacturing. *Addit. Manuf.* **2020**, *36*, 101569. [CrossRef]
4. Kumarage, H.; Khalil, I.; Tari, Z.; Zomaya, A. Distributed anomaly detection for industrial wireless sensor networks based on fuzzy data modelling. *J. Parallel Distrib. Comput.* **2013**, *73*, 790–806. [CrossRef]
5. Raza, M.; Aslam, N.; Le Minh, H.; Hussain, S.; Cao, Y.; Khan, N.M. A Critical Analysis of Research Potential, Challenges, and Future Directives in Industrial Wireless Sensor Networks. *IEEE Commun. Surv. Tutor.* **2017**, *20*, 39–95. [CrossRef]
6. Jan, B.; Farman, H.; Javed, H.; Montrucchio, B.; Khan, M.; Ali, S. Energy Efficient Hierarchical Clustering Approaches in Wireless Sensor Networks: A Survey. *Wirel. Commun. Mob. Comput.* **2017**, *2017*, 6457942. [CrossRef]
7. Rostami, A.S.; Badkoobe, M.; Mohanna, F.; Keshavarz, H.; Hosseinabadi, A.A.R.; Sangaiah, A.K. Survey on clustering in heterogeneous and homogeneous wireless sensor networks. *J. Supercomput.* **2018**, *74*, 277–323. [CrossRef]
8. Xu, Y.; Wang, Q.; Xu, Y.; Liu, J.; He, C. MPDMAC-SIC: Priority-based distributed low delay MAC with successive interference cancellation for multi-hop industrial wireless networks. *Comput. Commun.* **2020**, *154*, 48–57. [CrossRef]
9. Liu, M.; Yang, K.; Zhao, N.; Chen, Y.; Song, H.; Gong, F. Intelligent Signal Classification in Industrial Distributed Wireless Sensor Networks Based Industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *17*, 4946–4956. [CrossRef]
10. Borgiani, V.; Moratori, P.; Kazienko, J.F.; Tubino, E.R.R.; Quincozes, S.E. Toward a Distributed Approach for Detection and Mitigation of Denial-of-Service Attacks within Industrial Internet of Things. *IEEE Internet Things J.* **2020**, *8*, 4569–4578. [CrossRef]
11. Cao, B.; Zhao, J.; Lv, Z.; Liu, X.; Kang, X.; Yang, S. Deployment optimization for 3D industrial wireless sensor networks based on particle swarm optimizers with distributed parallelism. *J. Netw. Comput. Appl.* **2018**, *103*, 225–238. [CrossRef]
12. Gholami, M.; Taboun, M.; Brennan, R. An ad hoc distributed systems approach for industrial wireless sensor network management. *J. Ind. Inf. Integr.* **2019**, *15*, 239–246. [CrossRef]
13. Zhong, J.; Zhang, F.; Yang, S.; Li, D. Restoration of interdependent network against cascading overload failure. *Phys. A Stat. Mech. Appl.* **2019**, *514*, 884–891. [CrossRef]
14. Ren, W.; Wu, J.; Zhang, X.; Lai, R.; Chen, L. A Stochastic Model of Cascading Failure Dynamics in Communication Networks. *IEEE Trans. Circuits Syst. II Express Briefs* **2018**, *65*, 632–636. [CrossRef]
15. Shen, Y.; Ren, G.; Ran, B. Cascading failure analysis and robustness optimization of metro networks based on coupled map lattices: A case study of Nanjing, China. *Transportation* **2021**, *48*, 537–553. [CrossRef]
16. Vivek, S. Cascading Failure from Targeted Road Network Disruptions. *arXiv* **2020**, arXiv:2010.09887.
17. Shen, Y.; Ren, G.; Ran, B. Analysis of cascading failure induced by load fluctuation and robust station capacity assignment for metros. *Transp. A Transp. Sci.* **2021**, 1942304. [CrossRef]
18. Liao, W.; Salinas, S.; Li, M.; Li, P.; Loparo, K.A. Cascading Failure Attacks in the Power System: A Stochastic Game Perspective. *IEEE Internet Things J.* **2017**, *4*, 2247–2259. [CrossRef]
19. Guo, H.; Zheng, C.; Iu, H.H.-C.; Fernando, T. A critical review of cascading failure analysis and modeling of power system. *Renew. Sustain. Energy Rev.* **2017**, *80*, 9–22. [CrossRef]
20. Zhao, Z. Research on Invulnerability of Wireless Sensor Networks Based on Complex Network Topology Structure. *Int. J. Online Eng.* **2017**, *13*, 100. [CrossRef]
21. Tan, X.; Tang, J.; Yu, L.; Wang, J. A New Energy-Efficient and Fault-Tolerant Evolution Model for Large-Scale Wireless Sensor Networks Based on Complex Network Theory. *Int. J. Distrib. Syst. Technol.* **2019**, *10*, 21–36. [CrossRef]
22. Liu, H.-R.; Dong, M.-R.; Yin, R.-R.; Han, L. Cascading failure in the wireless sensor scale-free networks. *Chin. Phys. B* **2015**, *24*, 050506. [CrossRef]
23. Fu, X.; Yao, H.; Yang, Y. Cascading failures in wireless sensor networks with load redistribution of links and nodes. *Ad Hoc Netw.* **2019**, *93*, 101900. [CrossRef]
24. Wang, T.; Zhang, Z.; Shao, F. Survivability Analysis on a Cyber-Physical System. *Machines* **2017**, *5*, 17. [CrossRef]
25. Guo, Z.; Wang, Y.; Zhong, J.; Fu, C.; Sun, Y.; Li, J.; Chen, Z.; Wen, G. Effect of load-capacity heterogeneity on cascading overloads in networks. *Chaos Interdiscip. J. Nonlinear Sci.* **2021**, *31*, 123104. [CrossRef]
26. Fan, C.; Wang, B.; Tian, J. Cascading failure model in aviation network considering overload condition and failure probability. *J. Comput. Appl.* **2022**, *42*, 502. [CrossRef]
27. Zhong, J.; Sanhedrai, H.; Zhang, F.; Yang, Y.; Guo, S.; Yang, S.; Li, D. Network endurance against cascading overload failure. *Reliab. Eng. Syst. Saf.* **2020**, *201*, 106916. [CrossRef]
28. Wang, B.; Zhang, Z.; Qi, X.; Liu, L. Identify Critical Nodes in Network Cascading Failure Based on Data Analysis. *J. Netw. Syst. Manag.* **2020**, *28*, 21–34. [CrossRef]
29. Potts, M.W.; Sartor, P.A.; Johnson, A.; Bullock, S. A network perspective on assessing system architectures: Robustness to cascading failure. *Syst. Eng.* **2020**, *23*, 597–616. [CrossRef]
30. Lei, W.; Ma, J.; Ma, S. Robustness analysis of scale-free networks against cascading failures with tunable redistribution load parameters. In Proceedings of the 2021 China Automation Congress (CAC), Beijing, China, 22–24 October 2021; pp. 2908–2911. [CrossRef]

31. Hou, Y.; Xing, X.; Li, M.; Zeng, A.; Wang, Y. Overload cascading failure on complex networks with heterogeneous load redistribution. *Phys. A Stat. Mech. Appl.* **2017**, *481*, 160–166. [CrossRef]
32. Xiao, X.; Joshi, S.; Cecil, J. Critical assessment of Shape Retrieval Tools (SRTs). *Int. J. Adv. Manuf. Technol.* **2021**, *116*, 3431–3446. [CrossRef]
33. Zhang, L.; Xia, J.; Cheng, F.; Qiu, J.; Zhang, X. Multi-Objective Optimization of Critical Node Detection Based on Cascade Model in Complex Networks. *IEEE Trans. Netw. Sci. Eng.* **2020**, *7*, 2052–2066. [CrossRef]
34. Liu, C.; Li, D.; Fu, B.; Yang, S.; Wang, Y.; Lu, G. Modeling of self-healing against cascading overload failures in complex networks. *Eur. Lett.* **2014**, *107*, 68003. [CrossRef]
35. Shen, Y.; Ren, G.; Zhang, N.; Song, G.; Wang, Q.; Ran, B. Effects of mutual traffic redistribution on robustness of interdependent networks to cascading failures under fluctuant load. *Phys. A Stat. Mech. Appl.* **2020**, *560*, 125138. [CrossRef]
36. Qi, X.; Yang, G.; Liu, L. Robustness analysis of the networks in cascading failures with controllable parameters. *Phys. A Stat. Mech. Appl.* **2020**, *539*, 122870. [CrossRef]
37. Liu, X. Atypical Hierarchical Routing Protocols for Wireless Sensor Networks: A Review. *IEEE Sensors J.* **2015**, *15*, 5372–5383. [CrossRef]
38. Ávila, K.; Sanmartin, P.; Jabba, D.; Gómez, J. An analytical Survey of Attack Scenario Parameters on the Techniques of Attack Mitigation in WSN. *Wirel. Pers. Commun.* **2021**, 1–32. [CrossRef]
39. Chattopadhyay, S.; Dai, H.; Eun, D.Y. Maximization of Robustness of Interdependent Networks Under Budget Constraints. *IEEE Trans. Netw. Sci. Eng.* **2019**, *7*, 1441–1452. [CrossRef]
40. Shi, X.; Deng, D.; Long, W.; Li, Y.; Yu, X. Research on the robustness of interdependent supply networks with tunable parameters. *Comput. Ind. Eng.* **2021**, *158*, 107431. [CrossRef]
41. Fu, X.; Yang, Y. Modeling and analyzing cascading failures for Internet of Things. *Inf. Sci.* **2021**, *545*, 753–770. [CrossRef]