Hindawi
Wireless Communications and Mobile Computing
Volume 2020, Article ID 4617239, 11 pages
https://doi.org/10.1155/2020/4617239

Research Article

Quantitative Invulnerability Analysis of Artificial Spider-Web Topology Model Based on End-to-End Delay

Jun Wang[1,2] **Zhuangzhuang Du**[1] **and Zhitao He**[1]

[1]*College of Agriculture Equipment Engineering, Henan University of Science and Technology, Luoyang, Henan 471003, China*
[2]*Collaborative Innovation Center of Machinery Equipment Advanced Manufacturing of Henan Province, Luoyang, Henan 471003, China*

Correspondence should be addressed to Zhuangzhuang Du; dzzwq123521@163.com

Received 30 May 2019; Accepted 28 January 2020; Published 18 February 2020

Academic Editor: Davide Mattera

This paper presents an artificial spider-web topology model inspired by the structure and invulnerability of a spider web. A hierarchical clustering routing rule is accordingly established using the vibration transmission features of the natural spider web as a reference. Furthermore, the end-to-end delay is applied as the quantitative indicator of invulnerability for analyzing the communication performance and characteristics of the artificial spider-web topology. The simulation tests of a one-layer and 3-layer artificial spider-web model are implemented to obtain the importance and destructive tolerance of network components based on OPNET, with the change of communication conditions and fault types. This paper can provide a practical analysis method for the invulnerability of the artificial spider-web topology and offer important implications for the construction and maintenance of wireless sensor networks based on the topology.

1. Introduction

Wireless sensor network (WSN) is a multihop ad hoc network system that is formed as a result of communication among a large number of sensor nodes deployed in a target area, which is an important technical form of the underlying network of the Internet of things [1]. Adopting the monitoring method with the application of WSNs is suitable for many fields, such as object locations on a battlefield, the collection of physiological data, intelligent transportation systems, and ocean exploration [2]. However, the WSN often encounters node failures, routing failures, and communication interruptions due to energy exhaustion, hardware failure, and so on, which cause the segmentation of the connected network topology, the shrinkage of coverage, and even the damage to the whole network [3]. Therefore, how to enhance the invulnerability of the WSN is an important research field for the realization of its monitoring functions.

In recent years, topology control technology has become a hot subject in the study on WSN invulnerability [4]. The current studies mainly focus on scale-free models [5–7]. Based on the Barabási–Albert (BA) scale-free model, Chen et al. proposed the B model, where an increase in nodes and links and link deletion mechanisms conform to the actual network characteristic that the network size changes over time [8]. Although the foregoing research has made some prospective progress, the assumption of the network model is excessively ideal. For example, the assumptions of accurate locating, even distribution, strict synchronization, and so on of sensor nodes fail to account for a large number of difficulties found in practical applications [9]. Therefore, a more practical topology model should be built. At present, some researchers have begun to apply bioinspired network topology models to improve the network invulnerability [10]. Applications of the bionic network topologies exhibit enormous potential value for WSN development. Charalambous et al., based on the lateral suppression principle, proposed an energy-efficient topology management model that is inspired by the signal transmission patterns of biological intercellular communication, and they simulated the induction algorithm on size-limited networks. The results show that the energy efficiency can be improved by building

compact clusters in the clustering stage of the model [11]. Jun studied invulnerability of molecular structures of adenylate kinase and its relationship with the rigidity of spatial structures. The results show that the atomic topological structure preserves the rigid information of the protein molecular structure, and the invulnerability is strongly associated with the rigidity of spatial structures through measurements of natural connectivity [12]. The above-mentioned network models are too complex and difficult to establish, especially in the case of a large-scale sensor node deployment where they cannot secure the quality of communication. A simple and stable network model with high communication quality is more suitable for deployment in reality.

A spider web is a special structure that combines elegance, nature, and ultralightness. Its simple, stable, yet highly tough structure is extremely inspirational for research on WSN invulnerability. Spider webs can be divided into several types, such as the sheet web, dish web, irregular web, and orb-web. Orb-webs have a special status in spider-web evolution, and their structure is simple and regular, and thus, studies on spider webs are mostly concentrated on orb-webs [13]. The network topology of a typical orb-web has much similarity to a WSN model. Some researchers have started initial research on the topology of artificial spider-web network models. From the structure and durability of spider webs, Xiaosheng et al. proposed a new PLC network model and discussed the characteristics of the model and the process in which a low-voltage power distribution network transforms from a physical topology to an artificial spider-web logic topology. They proved that the new network model has advantages in improving the reliability of the PLC network communication [14]. Jun et al. established a mathematical model of artificial spider webs and concluded that the network structure of an artificial spider web is superior to that of a traditional network in terms of the improvement in the reliability and invulnerability of communication systems [15]. Yuh-Shyan et al. established multiple wireless M2M (machine-to-machine) dynamic spider-web network topologies based on the spider-web network topology to extend the network's lifetime by dynamically adjusting different sub-spider-web sizes [16]. As a concrete measure of network performance, we could make an accurate assessment of the invulnerability of the artificial spider-web topology model. Meanwhile, we could also evaluate the effectiveness by using the topology model to improve the network invulnerability. However, current studies have merely made related exploration of the invulnerability of the topology model through the quantitative analysis method, and the existing research only makes a preliminary exploration of the invulnerability of the spider-web structure model and does not carry out quantitative analysis of the invulnerability of the network topology model based on the in-depth summary of spider-web structure characteristics. Sergey et al. studied the cascading failure problem of interdependent networks based on the above research [17]. Jingxia and Junjie investigated the dynamic model of heterogeneous wireless sensor networks in order to balance the energy consumption of nodes and prolong the network life [18]. However, the model construction and analysis method driven by scenario adaptability is difficult to analyze the invulnerability of the proposed artificial spider-web model. Therefore, in view of the structural characteristics of the spider-web network, it is urgently needed to put forward an effective analysis approach.

OPNET is a powerful network design and simulation tool that has been widely used in industry and academia [19, 20]. OPNET offers precise analysis of the performance and behavior of complex networks and can be used for accurate descriptions of network invulnerability. Furthermore, there are plenty of available parameters used to characterize the network invulnerability numerically at present, such as degree, proximity, betweenness, shortest path, and minimum spanning tree. Nevertheless, these parameters cannot directly reflect the network invulnerability, which only focus on describing the changes in the network topology structure. The change of data transmission performance before and after network destruction is the intuitive reflection of network invulnerability. The parameter of end-to-end delay can be applied to characterize the importance and destructive tolerance of the components (e.g., node and communication link) in the network. The main objective of this study is to perform evaluation analysis of the invulnerability of the artificial spider-web topology model through a series of simulation experiments based on OPNET software. Specifically, we use the software tool to simulate different communication conditions (channel noise, packet interval, and random seed) and different degrees and types of link or node failures and adopt end-to-end delay as the indicator to depict the network invulnerability. This study can lay a solid foundation for building an analytical model of invulnerability of the WSN inspired by a spider web with the help of theories and methods such as probability theory and graph theory.

2. Materials and Methods

2.1. Artificial Spider-Web Topology Modeling. The structure of the orb-web (Figure 1) is composed of dragline threads and capture threads. According to varied functions, the dragline thread can be divided into three types: frame thread, anchor thread, and radiating thread. The frame threads are located on the periphery of the spider web to build a framework for the whole spider web. The anchor threads are the net frame for fixing the whole spider web. The radiating threads radiate outward from the central area and connect with the frame threads to maintain and support the stability of the whole spider-web structure. The central area is located in the center of the orb-web. The capture threads present a spiral structure woven outward rotationally from the central area. A cell is a grid space surrounded by two adjacent radiating threads and two adjacent capture threads.

A typical orb-web structure is a special structure with an organic combination of star and ring topologies. The structural evolution of a spider web is illustrated in Figure 2, where Figure 2(a) is a star structure, Figure 2(b) is a ring structure, and Figure 2(c) is an artificial spider-web structure formed after evolution. A one-layer artificial spider-web

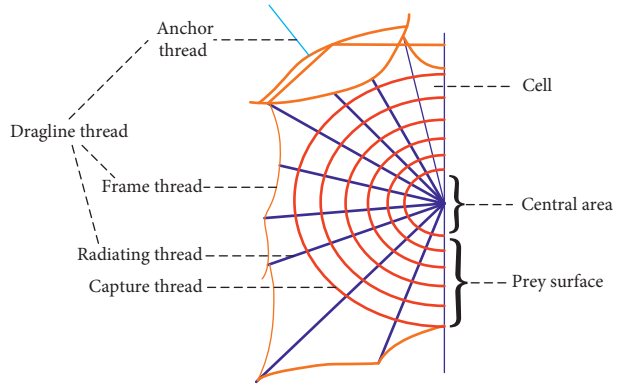

Figure 1: Orb-web structure.

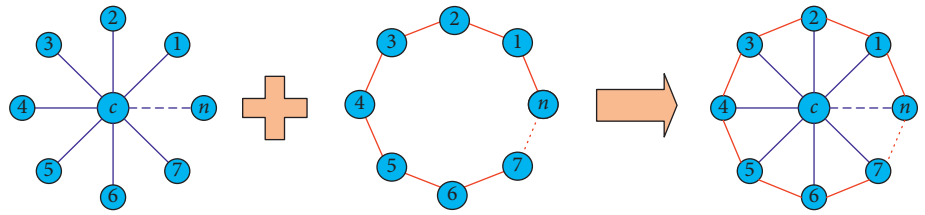

Figure 2: Evolution process of the spider-web structure (the letter c represents the central area, and the numbers from 1 to n denote child nodes).

structure can be obtained by means of a simple combination of a radial star structure and one-layer ring structure. The characteristics of the artificial spider-web topology are thus obtained as follows: (1) The artificial spider-web topology is the integration of a star topology and several ring topologies. Child nodes in the ring topology are also included in all of the child nodes in the star topology. (2) There is definitely a central area, which can be made of one or more nodes, and the center can establish a radial connection with all of the other child nodes. (3) In the same layer, chordwise connections can be established between child nodes, and each child node can establish up to two chordwise direct connection paths with adjacent child nodes.

To express the structural characteristics of the artificial spider web and provide a mathematical foundation for further research, this paper defines the parameters of the artificial spider-web topology (Figure 3) as follows:

(1) A center node is defined as the base station (BS), with n being the total number of nodes in one layer.

(2) The spider layers around the BS are represented by L. This parameter reflects the complexity and communication coverage of an artificial spider-web topology.

(3) The total number of nodes in an artificial spider-web topology is indicated by N, which has the following relationship with L and n:

$$N = L \times n. \tag{1}$$

(4) All nodes are numbered in turn along the direction of spiral magnification, and N_i refers to a certain node in an artificial spider-web topology, where $1 \le i \le N$.

(5) The communication link along the radial direction of an artificial spider-web topology is defined as the floating chain, represented by F_{p-q}. The definition of a floating chain falls into two cases: (1) In the case in which a node has a direct connection with the BS, p = BS and $1 \le q \le n$, in which q represents a certain node in the first layer that is radially connected to the BS. (2) In the case of radial connections between two nodes in adjacent layers, $p = i$ and $q = i - n$, where p is a node in an artificial spider-web topology except nodes in the first layer and q is an adjacent inner-layer node radially connected with it.

(6) The communication link along the chordwise direction of an artificial spider-web topology is defined as the string chain, represented by S_{j-f}. The definition of a string chain can be separated into two cases: (1) In the case in which a node on the first floating chain has a chordwise connection with a node on the nth floating chain, $j = kn + 1$ and $f = kn + n$, where j and f represent, respectively, the numbers of nodes in the same layer on the first and nth floating chains and k denotes a positive integer. (2) In the case of chordwise connections between the other adjacent nodes in the same layer, except for the nodes on the first floating chain, $j = I$ and $f = i - 1$, in which $1 < i \le N_n$ and $i \ne k_n + 1$.

(7) θ is the sector angle, namely, the angle between two adjacent floating chains:

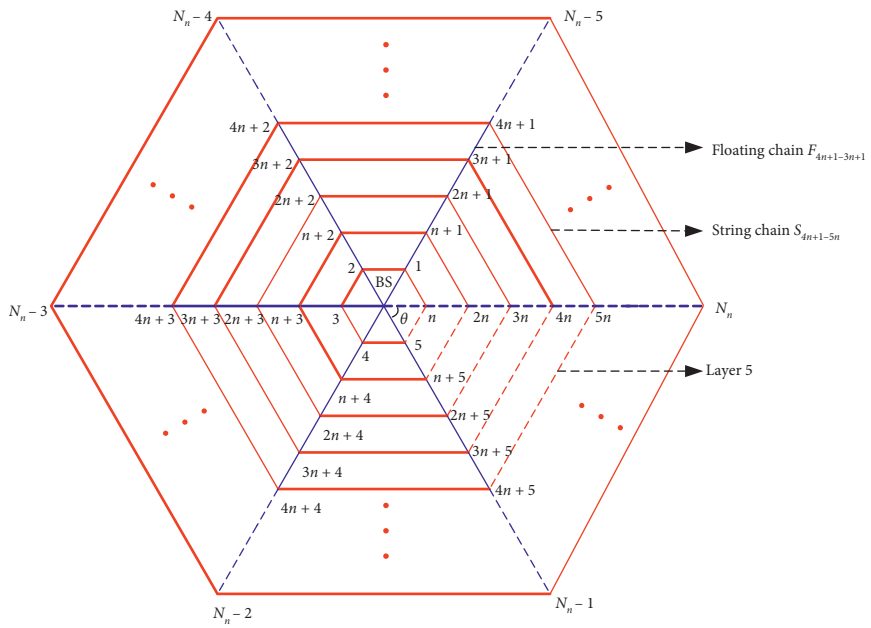

Figure 3: Parameters of the artificial spider-web topology.

$$\theta = \frac{360^{\circ}}{n}. \tag{2}$$

2.2. Artificial Spider-Web Routing Rule. Previous studies on the vibration transmissibility of a spider web have found that the vibration signals of the spider web are mainly transmitted through radiating threads, while the capture threads only undertake a small amount of the vibration [21, 22]. Based on the artificial spider-web topology, we use the vibration transmission characteristics of the natural spider web for reference to establish a hierarchical clustering routing rule. The specific routing rule is as follows.

2.2.1. Selection of Cluster Heads. To avoid the communication overhead caused by frequent elections of cluster heads and guarantee the uniform distribution of cluster heads, we assign the first-layer nodes $N_1 - N_n$ connected with the BS as cluster heads.

2.2.2. Determination of a Cluster Member. In the initial stage of the network construction, the minimum hops to the BS are obtained for each isolated node based on the flood routing algorithm, and the routing table of the minimum hops is established. All these nodes are arranged hierarchically with the minimum hops, and the nodes with the equal quantity of hops are classified into the same layer. Furthermore, the nodes connected with a cluster head N_i $(1 \le i \le n)$ in different layers by the minimum hops are categorized as the member nodes of the cluster head. After all nodes are sorted into clusters, the nodes in each individual cluster obviously constitute an independent radial link.

2.2.3. Communications between Cluster Heads and BS. According to the artificial spider-web topology, a cluster head directly connects with the BS, two adjacent cluster heads, and a cluster member node. Each cluster head receives the data of all cluster member nodes and forwards to the BS. Once a link failure occurs between a cluster head and the BS or the radial link flow between the cluster head and the BS exceeds the threshold Y, an adjacent cluster head node is selected as the relay node in the specified order for data transmit.

2.2.4. Data Transmission between Cluster Member Nodes and Cluster Head. Cluster member nodes convey data to the corresponding cluster head in the form of multihop in accordance with the principle of shortest path priority, and then the cluster head transfers the data to the BS. If the link traffic in the shortest path exceeds the threshold Y or the node or link fails, adjacent link nodes in the same layer can be selected in turn as relay nodes to send data to the adjacent cluster head and further deliver to the BS, which is consistent with the routing rule in case of cluster-head failure.

The steps of the hierarchical clustering routing rule are summarized in Algorithm 1.

2.3. Invulnerability Analysis Method and Parameter Settings. Numerous studies have shown that the spider web presents excellent biological characteristics, such as having a simple and light structure, high mechanical strength, and strong energy dissipation [23–25]. However, the related study on invulnerability analysis of the artificial spider-web topology still remains in the initial stage. End-to-end delay is the duration between the time that a source node produces a data packet and the time that this packet reaches its destination node, which is the direct reflection of influence on communication caused by network component failure. We use end-to-end delay as the indicator to evaluate the invulnerability of the artificial spider-web topology. The concrete definition of end-to-end delay is as follows: the

Input: the node N_i, the total number of nodes in one layer n, the total number of nodes in the artificial spider-web topology N, and the threshold Y
Output: routing path from the node N_i to the BS
(1) /∗ Communication between nodes located from the 2nd layer to the outermost layer and BS∗/
(2) **while** $n < i \le N$ **do**
(3) **for** N_i, $n < i \le N$ **do**
(4) **if** no link failure exists between N_i and N_{i-n}, and link traffic does not exceed the threshold value Y
(5) **then** N_i forwards data to N_{i-n}
(6) **end for**
(7) **for** $i = (k+1) * n$, $1 \le k \le N/n$ **do**
(8) $N_{(k+1)n}$ transfers data to $N_{(k+1)n-1}$
(9) **if** $N_{(k+1)n-1}$ fails
(10) **then** $N_{(k+1)n}$ transmits data to $N_{(k+1)n+1}$
(11) **end for**
(12) **for** $i = kn + 1$, $1 \le k \le N/n$ **do**
(13) N_{kn+1} delivers data to N_{kn+n}
(14) **if** N_{kn+n} undergoes a failure
(15) **then** N_{kn+1} passes data to N_{kn+2}
(16) **end for**
(17) **for** $i \ne (k+1) * n$且$i \ne kn+1$, $1 \le k \le N/n$ **do**
(18) N_i sends data to N_{i-1}
(19) **if** N_{i-1} is out of order
(20) **then** N_i conveys data to N_{i+1}
(21) **end for**
(22) **end while**
(23) **break**;
(24) /∗Communication between the first-layer nodes and BS∗/
(25) **if** $1 = < i \le n$
(26) **then** N_i is a cluster head
(27) **if** no link failure exists between N_i and BS, and link traffic does not exceed the threshold value Y
(28) **then** N_i forwards data to BS
(29) **else** judge the value of i
(30) **if** $i = 1$
(31) **then** N_1 sends data to N_n and forwards them to the BS along N_n's radial link further. In case of N_n failure, N_1 transmits data to N_2 and then passes them to the BS by the radial link through N_2
(32) **else if** $i = n$
(33) **then** N_n transmits data to N_{n-1} and forwards them to the BS by N_{n-1}'s radial link. If N_{n-1} fails, N_n transfers data to N_1 and then delivers them to the BS along the radial link through N_1
(34) **else** N_i conveys data to N_{i-1} and forwards them to the BS via N_{i-1}'s radial link. If N_{i-1} malfunctions, N_i sends data to N_{i+1} and then transfers them to the BS along the radial link through N_{i+1}
(35) **end if**
(36) **end if**
(37) **end if**

ALGORITHM 1: Hierarchical clustering routing rule.

delay time for any node N_i to send the data packet to the BS is T_i, in which $1 \le i \le N_n$; the total end-to-end delay for all nodes is $T_n = \sum_{i=1}^{N_n} T_i$; the end-to-end delay E_d is defined as the ratio between the total delay time in which all nodes send the data packet to the BS and N_n, which is expressed as

$$E_d = \frac{T_n}{N_n}. \tag{3}$$

Moreover, we choose a one-layer and 3-layer artificial spider web as studying objects in order to analyze the invulnerability rule. The parameters of the one-layer artificial spider-web model are the sector angle $\theta = 60^\circ$ and 6 nodes. For the 3-layer artificial spider web, the parameters are the sector angle $\theta = 60^\circ$ and 18 nodes. A total of 3 sets of simulation tests are conducted on the one-layer artificial spider-web model, which specifically include (1) the end-to-end delay test of the topology model with/without noise; (2) the end-to-end delay test of the topology model with different packet intervals; and (3) the end-to-end delay test of the topology model with different random seeds. These tests are for analyzing the influence of different external or internal conditions on the communication performance of the artificial spider-web topology. Two sets of simulation tests are conducted on the 3-layer artificial spider-web model, which specifically include the following: (1) the end-to-end delay test for damage to a single radial link and single node layer by layer and (2) the end-to-end delay test for damage to the same layer of nodes and links. The two sets of tests are

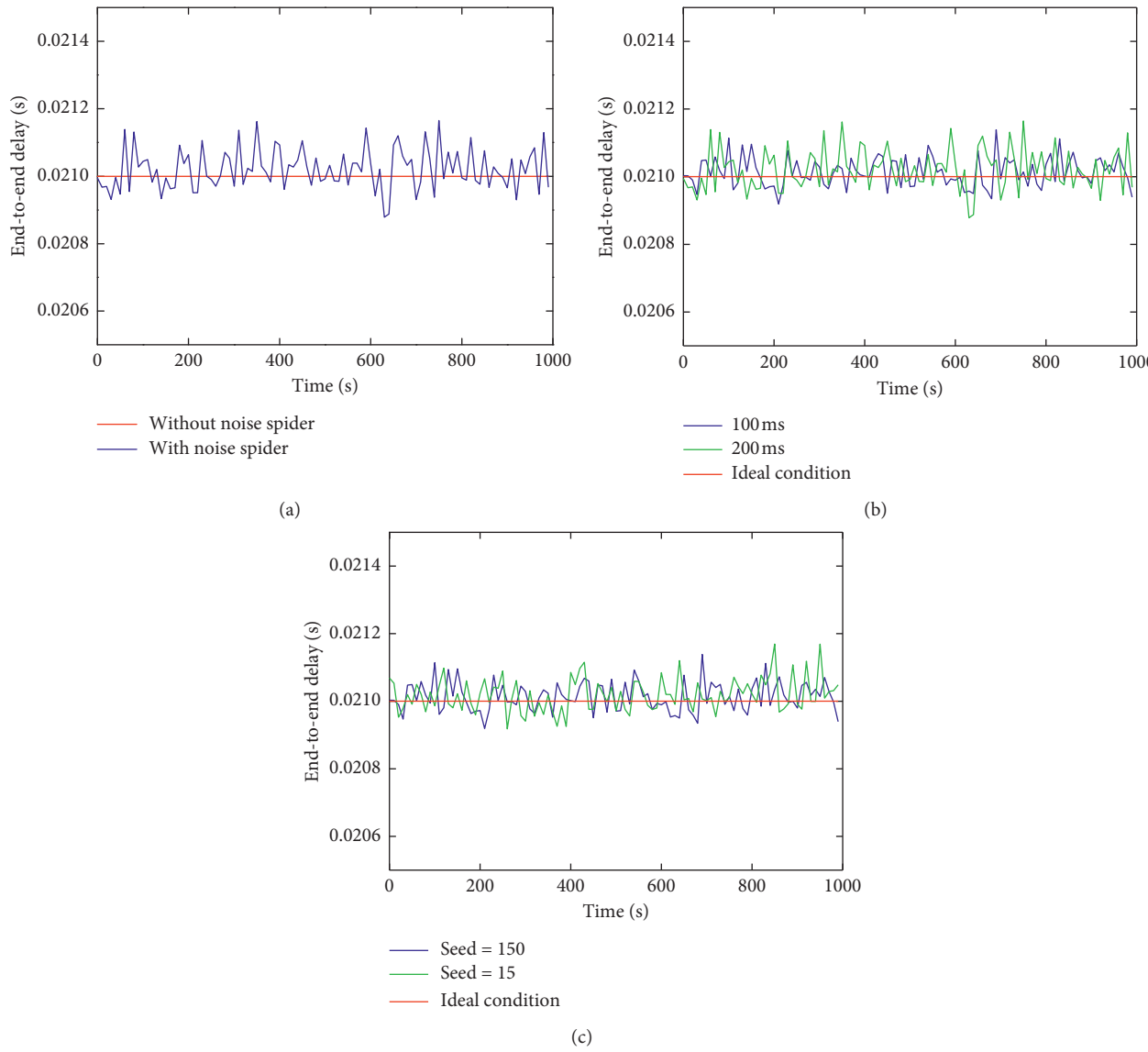

Figure 4: Simulation results of the end-to-end delay time of the one-layer artificial spider-web topology under different conditions. (a) Noise (with, without). (b) Packet interval (200 ms, 100 ms). (c) Random seed (15, 150).

used to analyze the difference in network communication performance before and after the artificial spider-web topology damaged.

OPNET (Optimized Network Engineering Tool) provides a comprehensive development environment for the specification, simulation, and performance analysis of communication networks. A large range of communication systems from a single WSN to global satellite networks can be supported. In this paper, we apply OPNET 14.5 as the simulation platform to perform the analysis of the invulnerability of the artificial spider-web topology model. The simulation process defines three packet formats, namely, data packet, broadcast packet, and noise packet. The data packet size is defined as 200 bit, and that of the broadcast packet and noise packet is 72 bit; the bandwidth of the link is defined as 9600 bps, with a simulation time set to 1000 s and the default peripheral node's packet interval set to 0.1 s.

3. Results and Discussion

3.1. One-Layer Artificial Spider-Web Topology. The communication conditions of the WSN have a massive influence on the stability of the network. On the one hand, the network channel is sensitive to channel noise interference, causing channel imbalance and increasing the probability of packet loss. On the other hand, the packet interval directly affects the establishment time of network routing, control overhead, and transmission delay. In addition, network communication has significant uncertainties and randomness. In order to assess the communication stability of the artificial spider-web topology model, we conducted the following three groups of simulation tests.

Figure 4(a) shows the waveform variation of the end-to-end delay of the one-layer artificial spider-web topology without and with noise. Without noise, the time delay is

maintained at 0.021 s (ideal end-to-end delay before adding noise). After the addition of random noise between 100 ms and 500 ms, the delay fluctuates, and the peak value difference in the delay fluctuation is 0.0003 s, which accounts for 1.59% of the average time delay and is basically consistent with that without noise. The waveform variation of the end-to-end delay of the one-layer artificial spider-web topology is demonstrated in Figure 4(b), where the noise conditions stay the same and the packet intervals are, respectively, 200 ms and 100 ms. Both the end-to-end delay curves fluctuate around the ideal end-to-end delay. When the packet interval is 200 ms, the maximum increase of amplitude is 0.66% and the minimum decrease of amplitude is 0.38%. When the packet interval is 100 ms, the maximum increase of amplitude is 0.78% and the minimum decrease of amplitude is 0.57%. The results indicate that the packet interval produces a very small impact on the one-layer artificial spider-web topology. Figure 4(c) shows the waveform variation of the end-to-end delay of the one-layer artificial spider-web topology over time, where the noise conditions remain unchanged and the random seeds are 15 and 150, respectively. When the random seed is 15, the maximum increase of amplitude is 0.80% and the minimum decrease of amplitude is 0.39%. When the random seed is 150, the maximum increase of amplitude is 0.66% and the minimum decrease of amplitude is 0.38%. The results show that the delay fluctuation against different noise conditions, packet intervals, and random seeds all goes below 1.6% of the ideal end-to-end delay; thus, noise, packet interval, and random seed have comparatively small influence on the network transmission capability of the one-layer artificial spider-web topology. The topology presents strong reliability and stability, which can meet the service quality of wireless sensor networks.

3.2. 3-Layer Artificial Spider-Web Topology

3.2.1. End-To-End Delay Test for Damage to a Single Radial Link and Single Node Layer by Layer. Aiming at achieving the impact of the damage of links in varied layers along the same radial line on the end-to-end delay of the topology, simulation tests with a complete network and damaged links $F_{c\text{-}2}$, $F_{8\text{-}2}$, and $F_{14\text{-}8}$ are conducted in turn. The damaged links are shown in Figure 5. Figure 6 presents the simulation results. By comparison with the complete network, it can be seen that, in the case of damage to links $F_{c\text{-}2}$, $F_{8\text{-}2}$, and $F_{14\text{-}8}$, the delay in turn increases by 23.3%, 11.6%, and 2.3%, respectively, which shows that the impact of the inner links on the invulnerability is greater than that of the outer links. From the above analysis, it can be clarified that when the radial link is damaged, the outer node and inner node cannot directly transmit data but communicate with the inner node through the relevant relay node according to the hierarchical clustering routing rule. As a result, the number of links that undertake data transmission inevitably increases and the network delay also raises correspondingly. Furthermore, the closer the link to the BS on the same radial line is damaged, the longer the end-to-end delay is, indicating the higher importance of the link.

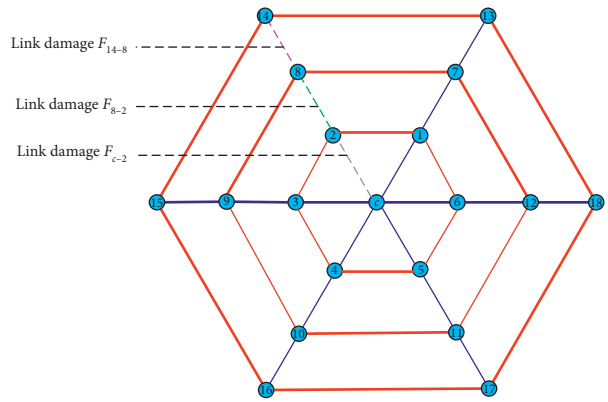

Figure 5: Layer-by-layer damage of the radial links $F_{c\text{-}2}$, $F_{8\text{-}2}$, and $F_{14\text{-}8}$.

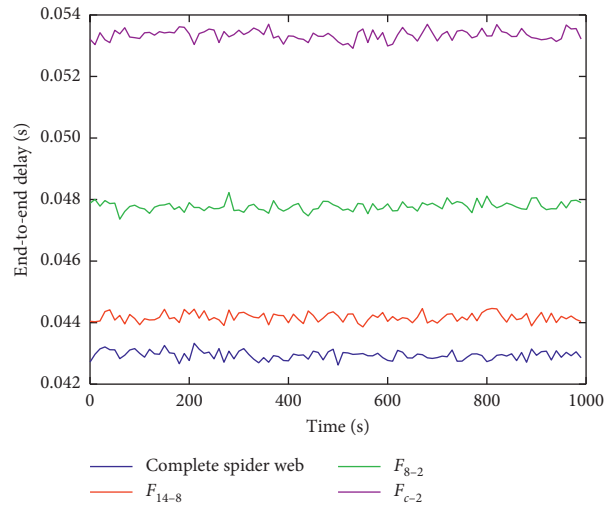

Figure 6: Simulation results of the end-to-end delay in the case of damage in the radial links in different layers.

Some nodes in the topology are responsible for a large amount of data send-receive assignment, which have more important value than other nodes. Whether these nodes operate normally or not directly affects the performance of the network. Therefore, verifying the importance of nodes in the network has certain significance for improving the survivability of the entire communication network. In order to analyze the importance of the nodes in varied layers along the same radial line by the end-to-end delay of the network, simulation tests of the complete network and damage to nodes N_2, N_8, and N_{14} are conducted. The damaged nodes are depicted in Figure 7.

Figure 8 shows the simulation results of the 3-layer artificial spider-web model in the case of the complete network and damage to N_2, N_8, and N_{14}. When nodes N_2 and N_8 are damaged, the network delay is, respectively, 14.0% and 2.3% higher than the delay of the complete network. When the outermost node N_{14} is damaged, the network delay is 2.3% lower than the delay of the complete network, which indicates that while the inner-layer node damage extends the network delay, the outermost node damage

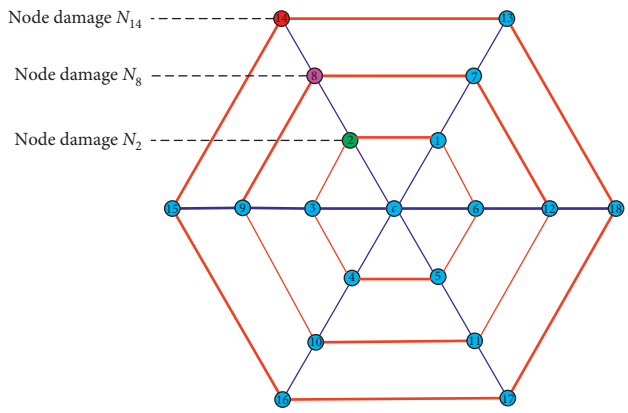

Figure 7: Layer-by-layer damage of the radial link nodes N_2, N_8, and N_{14}.

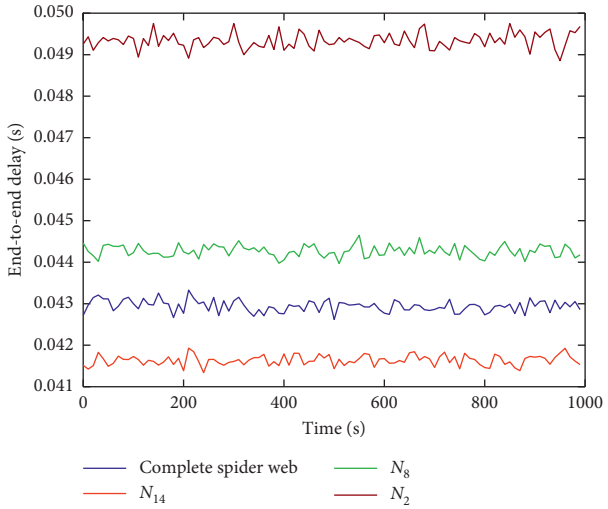

Figure 8: Simulation results of the end-to-end delay in the case of damage to nodes in different layers.

reduces the network delay. Consequently, the inner nodes are more important. Moreover, it can be seen from the analysis that the damage of a node will lead to the failure of communication links connected with it. The outer nodes accordingly need to establish communication link with the inner nodes through relay nodes, which inevitably increase network delay. However, when the outermost nodes are damaged, due to the fact that they are not responsible for forwarding data, the delay is not generated, and the end-to-end delay is slightly reduced compared to that of the complete network.

3.2.2. End-To-End Delay Test for Damage to the Same Layer of Nodes and Links. The difference in the end-to-end delay time of the artificial spider-web topology is evaluated based on the node and link damage for the quantitative analysis of the invulnerability of the topology under the conditions of damages in the same layer.

Damage of the node or link in each layer can be divided into 10 situations. Figure 9 illustrates the 10 situations by taking the first-layer node/link damage as an example, as follows: damage of any 1 node/link (A), damage of 2 adjacent nodes/links (B), damage of 2 nonadjacent nodes/links (C), damage of 3 adjacent nodes/links (D), damage of 3 nodes/links with 2 of them being adjacent to each other (E), damage of 3 nonadjacent nodes/links (F), damage of 4 adjacent nodes/links (G), damage of 4 nodes/links with 3 of them being adjacent nodes/links (H), damage of 4 adjacent nodes/links with any two of them being adjacent nodes/links (I), and damage of 5 adjacent nodes/links (J).

Table 1 shows the simulation results of the end-to-end delay and delay increment when nodes in the first, second, and third layers are damaged. Table 1 shows that, with an increase in the number of radial nodes damaged, delay increments of the first and second layers also tend to go up. The end-to-end delay increment rises from 0.006 s to 0.11 s with the number of damaged nodes in the first layer being increased from 1 to 5, which is increased by 18.3 times. Meanwhile, the end-to-end delay increment rises from 0.001 s to 0.026 s with the number of damaged nodes in the second layer being increased from 1 to 5, which is increased by 26 times. When nodes in the inner layer are damaged, the smaller their distance to the BS, the greater the network delay increment, and the greater the impact on the artificial spider-web topology. For instance, one node in the first and second layers is damaged, and the end-to-end delay increments are, respectively, 0.006 s and 0.001 s.

Under the condition of the damage of nodes in the same layer, the greater the number of adjacent nodes, the greater the degree of impact. When the number of damaged nodes is 2, where two adjacent nodes and two nonadjacent nodes are damaged, the end-to-end delay increments of first-layer nodes are 0.019 s and 0.014 s, respectively, and the end-to-end delay increments of nodes in the second layer are, respectively, 0.004 s and 0.003 s. Therefore, the damage of adjacent nodes in the same layer will seriously affect the normal communication function of the topology network. In the case of the damage of the outermost nodes (third-layer nodes), the network delay decreases with the increase of the number of damaged nodes. When the same number of nodes is destroyed, whether the nodes are adjacent or not has no obvious effect on the network delay. The special rule presented by the outermost node is related to its location. The outermost node only transmits information to the inner node according to the routing rule, so if the number of outermost node damages increases, the network delay will be shorter than that of the complete network, indicating that the damage of the outermost node has little impact on network communication performance.

Table 2 shows the simulation results of the end-to-end delay and delay increment when radial links in the first, second, and third layers are damaged. Table 2 shows that when the number of damaged links in layers 1, 2, and 3 increases from 1 to 5, the end-to-end delay increment rises by 16, 14.6, and 19 times, indicating that the end-to-end delay increment shows an upward trend with the increase of the number of radial link failures in the same layer. When 3 radial links in the first, second, and third layers are damaged, it shows that when the same number of links is destroyed at

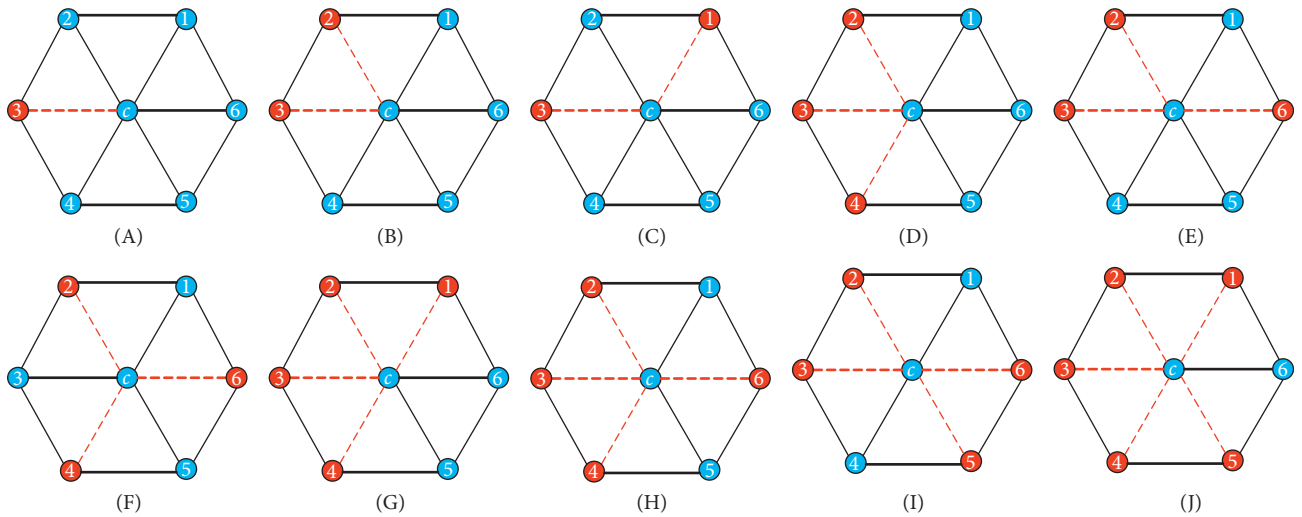

Figure 9: Fault types that may occur when the node/link is damaged in the first layer (the red solid circle represents the damaged nodes, and the red dotted line denotes the damaged links).

Table 1: Variation in the network delay when the nodes in the first, second, and third layers are damaged.

Number of nodes damaged	Failure type	End-to-end delay time (s)			Delay increment (s)		
		Damage of the 1st layer	Damage of the 2nd layer	Damage of the 3rd layer	Damage of the 1st layer	Damage of the 2nd layer	Damage of the 3rd layer
1	A	0.049	0.044	0.042	0.006	0.001	−0.001
2	B	0.062	0.047	0.040	0.019	0.004	−0.003
	C	0.057	0.046	0.040	0.014	0.003	−0.003
3	D	0.082	0.052	0.039	0.039	0.009	−0.004
	E	0.071	0.049	0.039	0.028	0.006	−0.004
	F	0.065	0.048	0.039	0.022	0.005	−0.004
4	G	0.112	0.059	0.037	0.069	0.016	−0.006
	H	0.093	0.054	0.037	0.050	0.011	−0.006
	I	0.087	0.053	0.037	0.044	0.010	−0.006
5	J	0.153	0.069	0.034	0.110	0.026	−0.009

Table 2: Variation in the network delay when links in the first, second, and third layers are damaged.

Number of radial links damaged	Failure type	End-to-end delay time (s)			Delay increment (s)		
		Damage of the 1st layer	Damage of the 2nd layer	Damage of the 3rd layer	Damage of the 1st layer	Damage of the 2nd layer	Damage of the 3rd layer
1	A	0.053	0.048	0.044	0.010	0.005	0.001
2	B	0.075	0.058	0.047	0.032	0.015	0.004
	C	0.064	0.053	0.045	0.021	0.010	0.002
3	D	0.107	0.072	0.050	0.064	0.029	0.007
	E	0.085	0.062	0.048	0.042	0.019	0.005
	F	0.074	0.057	0.047	0.031	0.014	0.004
4	G	0.149	0.092	0.055	0.106	0.049	0.012
	H	0.117	0.077	0.052	0.074	0.034	0.009
	I	0.106	0.072	0.050	0.063	0.029	0.007
5	J	0.203	0.116	0.062	0.160	0.073	0.019

different locations in the same layer, the larger the number of adjacent links, the greater the delay increment, and the effect of centralized damaged links on the invulnerability is greater than that of decentralized damaged links.

In the same circumstance, with the increase in the number of damaged layers, the end-to-end delay tends to decrease over time, and the increase in the network delay rapidly goes down. When 5 links in the first, second, and

third layers are damaged, the network delay increments are, respectively, 3.7, 1.7, and 0.44 times that of the complete network, which demonstrates that the impact of the inner links on the network delay is much greater than that of the outer links on the network delay.

Moreover, we can conclude that the importance distribution rule of nodes and links in the artificial spider-web topology model is as follows: (1) The nodes and links in the inner layers are much more important than the nodes and links in the outer layers. (2) Damage of adjacent links and nodes in the same layer is more likely to paralyze the topology network. (3) Damage of the outermost nodes reduces the coverage area of the model, but it has no impact on the proper communication of the inner layers. Through this analysis, it can be testified that the importance distribution rule of nodes is basically consistent with that of the links, so we should focus on maintenance of the nodes and links in inner layers in the network construction or enhance the network's invulnerability by increasing the deployment density of nodes at important places. Meanwhile, it is obviously an effective method to improve the fault tolerance ability of the artificial spider-web topology by reducing the possibility of simultaneous failures of adjacent nodes or links.

4. Conclusions

The spider-web structure is simple and lightweight; therefore, spiders can quickly capture the information on various objects slammed into the web; after sustaining the impact of large loads, the web can still maintain a powerful and effective connection. Local damage of a spider web does not affect the capture of prey and the transmission of vibration information. The structure of the spider web is somewhat similar to a WSN topology, and thus, the artificial spider-web topology is very inspirational for study on invulnerability. Inspired by specific advantages of the spider web, this paper establishes an artificial spider-web topology model, which defines the related structural parameters and takes the end-to-end delay as the indicator for describing the invulnerability performance of the topology. A series of simulation tests are conducted on a one-layer and 3-layer artificial spider-web model based on OPNET for the quantitative analysis. Analysis of simulation results shows the following: (1) The simulation results of the single-layer artificial spider web under different conditions show excellent network transmission stability and reliability. (2) Through the destruction of a single node, a single link, nodes, and links at the same time, and the destruction of different density under the same quantity, it is found that the importance of the location of the node and link is inversely proportional to the distance of the base station, and the denser the damage, the more serious the influence. (3) The invulnerability performance of the artificial spider-web topology under different communication conditions and different degrees and types of link or node failures is obtained, which provides a meaningful reference for extensive application of the spider web's advantageous characteristics for WSNs.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research activity described in this paper was jointly supported in part by the National Natural Science Foundation of China (Grant no. 61771184), Key Research Project of Education Bureau of Henan Province, China (Grant no. 17A416002), Key Scientific and Technological Project of Henan Province, China (Grant no. 172102210040), and Program for Science & Technology Innovation Talents in Universities of Henan Province (Grant no. 20HASTIT029). Finally, the authors would like to thank Dr. Jiajia Wang for her valuable suggestions on the research methods of this article.

References

[1] R. Krishnan and D. Starobinski, "Efficient clustering algorithms for self-organizing wireless sensor networks," *Ad Hoc Networks*, vol. 4, no. 1, pp. 36–59, 2006.

[2] G. Song, D. Xinwu, and Y. Jumei, "Study on measurement error of iron ore pipeline transportation flow based on weight function theory of electromagnetic flow sensor," *The Journal of Supercomputing*, vol. 75, no. 5, pp. 2289–2303, 2018.

[3] S. M. Zin, N. B. Anuar, M. L. M. Kiah et al., "Routing protocol design for secure WSN: review and open research issues," *Journal of Network and Computer Applications*, vol. 41, pp. 517–530, 2014.

[4] T. M. Chiwewe and G. P. Hancke, "A distributed topology control technique for low interference and energy efficiency in wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 8, no. 1, pp. 11–19, 2012.

[5] Z. Gengzhong and L. Qiumei, "Scale-free topology evolution for wireless sensor networks," *Computers & Electrical Engineering*, vol. 39, no. 6, pp. 1779–1788, 2013.

[6] Z. Gengzhong, L. Sanyang, and Q. Xiaogang, "Scale-free topology evolution for wireless sensor networks with reconstruction mechanism," *Computers and Electrical Engineering*, vol. 38, no. 3, pp. 643–651, 2012.

[7] N. Sarshar and V. Roychowdhury, "Scale-free and stable structures in complex ad hoc networks," *Physical Review. E, Statistical, Nonlinear, and Soft Matter Physic*, vol. 69, no. 2, Article ID 026101, 2004.

[8] C. Qinghua and S. Dinghua, "The modeling of scale-free networks," *Physica A: Statistical Mechanics and its Applications*, vol. 335, no. 1-2, pp. 240–248, 2004.

[9] L. Shudong, L. Lixiang, and Y. Yixian, "A local-world heterogeneous model of wireless sensor networks with node and link diversity," *Physica A: Statistical Mechanics and its Applications*, vol. 390, no. 16, pp. 1182–1191, 2011.

[10] W. Jiajia, Q. Zhihui, and R. Luquan, "Biomechanical comparison of optimal shapes for the cervical intervertebral fusion cage for C5-C6 cervical fusion using the anterior cervical plate and cage (ACPC) fixation system: a finite element analysis," *Medical Science Monitor*, vol. 7, no. 25, pp. 8379–8388, 2019.

[11] C. Charalambous and S. Cui, "A biologically inspired networking model for wireless sensor networks," *IEEE Network*, vol. 24, no. 3, pp. 6–13, 2010.

[12] W. Jun, T. Yuejin, D. Hongzhong et al., "Heterogeneity of scale-free network," *System Engineering Theory and Practice*, vol. 27, no. 5, pp. 101–105, 2007.

[13] B. J. Kaston, "The evolution of spider webs," *American Zoologist*, vol. 4, no. 2, pp. 191–207, 1964.

[14] L. Xiaosheng, Z. Liang, Z. Yan et al., "Performance analysis of power line communication network model based on spider web," in *Proceedings of the IEEE International Conference on Power Electronics and ECCE Asia*, Jeju, South Korea, June 2011.

[15] W. Jun, G. Song, H. Zhitao et al., "Research on artificial spider web model for farmland wireless sensor network," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6393049, 11 pages, 2018.

[16] Y.-S. Chen and W.-L. Chiang, "A spiderweb-based massive access management protocol for M2M wireless networks," *IEEE Sensors Journal*, vol. 15, no. 10, pp. 5765–5776, 2015.

[17] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 463, no. 7291, pp. 1025–1028, 2010.

[18] J. Zhang and J. Chen, "An adaptive clustering algorithm for dynamic heterogeneous wireless sensor networks," *Wireless Networks*, vol. 25, no. 1, pp. 455–470, 2017.

[19] E. Biegeleisen, M. Eason, C. Michelson et al., *Network in the Loop Using HLA, Distributed OPNET Simulations, and 3D Visualizations*, Military Communications Conference, Atlantic City, NJ, USA, 2005.

[20] M. S. Hasan, H. Yu, A. Griffiths et al., "Simulation of distributed wireless networked control systems over MANET using OPNET," in *Proceedings of the IEEE International Conference on Networking*, London, UK, April 2007.

[21] R. Das, A. Kumar, A. Patel, S. Vijay, S. Saurabh, and N. Kumar, "Biomechanical characterization of spider webs," *Journal of the Mechanical Behavior of Biomedical Materials*, vol. 67, pp. 101–109, 2017.

[22] H. Yu, J. Yang, and Y. Sun, "Energy absorption of spider orb webs during prey capture: a mechanical analysis," *Journal of Bionic Engineering*, vol. 12, no. 3, pp. 453–463, 2015.

[23] V. Tietsch, J. Alencastre, H. Witte, and F. G. Torres, "Exploring the shock response of spider webs," *Journal of the Mechanical Behavior of Biomedical Materials*, vol. 56, pp. 1–5, 2016.

[24] Z. Qin, B. G. Compton, J. A. Lewis et al., "Structural optimization of 3D-printed synthetic spider webs for high strength," *Nature Communications*, vol. 6, Article ID 7038, 2015.

[25] B. D. Opell and J. E. Bond, "Capture thread extensibility of orb-weaving spiders: testing punctuated and associative explanations of character evolution," *Biological Journal of the Linnean Society*, vol. 70, no. 1, pp. 107–120, 2000.