

Research Article

Reliability Analysis of Social Network Data Transmission in Wireless Sensor Network Topology

Zhixue Wang 

School of Mathematics and Computer Science, Ningxia Normal University, Guyuan Ningxia 756000, China

Correspondence should be addressed to Zhixue Wang; nxwzx@nxnu.edu.cn

Received 5 November 2021; Revised 6 December 2021; Accepted 10 December 2021; Published 6 January 2022

Academic Editor: Gengxin Sun

Copyright © 2022 Zhixue Wang. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, the reliability of data transmission in social networks is thoroughly studied and analyzed using wireless sensor network topology technology. This paper, based on the introduction of sensor network reliability analysis-related technology, combined with the characteristics, and needs of the sensor network itself, focuses on the study of the reliability analysis of the sensor network under the state of perturbation scheme. Based on the idea of making full use of data changes to respond to the sensor state, this paper takes the actual monitoring data of the wireless sensor network as the research object, selects the temporal correlation and spatial correlation of the measured environmental data as the reliability index by extracting the features of the wireless sensor network data, and proposes the Evidential reasoning rule- (ER-) based wireless sensor network data reliability assessment model based on Evidential reasoning rule (ER) is proposed. The data are mined, analyzed, and quantified from the perspective of content popularity, and the interest indicators of nodes on data under content popularity are analyzed to derive stable interest quantification values. Combined with the network properties, i.e., node autoassembly community, we analyze the data dissemination characteristics of social networks in wireless sensor network topology environment and derive the upper and lower bounds of data transmission capacity under node interest-driven and its variation on network performance. Social relationships among nodes affected by social attributes are considered; in turn, the data forwarding behavior of nodes is modeled using data transmission probability and data reception probability; finally, the data forwarding process is analyzed and a closed expression for the average end-to-end transmission capacity is derived in turn.

1. Introduction

With the development of technology, social networking applications such as Weibo, YouTube, and Twitter provide people with convenient ways to communicate. Traditional social media content is mainly in the form of pictures, articles, and so on. In recent years, with the development of cloud computing, the Internet of Things, and other technologies, various new social network applications represented by new media methods such as interactive live streaming and real-time meetings have started to appear in the users' view [1]. In such applications, users are more sensitive to the access delays of various new media. At the same time, the popularity of smart mobile devices has brought hundreds of millions of users to join social networking applications for real-time communication, and the amount of data generated by them has exploded, making it increasingly

important to maintain a reasonable load balance of storage systems to ensure good system performance. Although traditional social networking applications use cloud computing platforms to place user data in a way that can provide better storage services for massive amounts of user data, cloud data centers are generally far away from users, which makes it difficult to ensure users' high real-time requirements for various new social media [2]. With the development of wireless technology, the availability, coverage, and performance of wireless communication are rapidly improving, and it has become a necessity of modern life, which can effectively complete the various demands made by network users and is suitable for various long-range and short-range wireless transmissions. In addition, the shared and open nature of wireless propagation channels, which cannot simultaneously satisfy the service requests of many users, leads to lower communication quality and increases the complexity of

wireless transmission, while secure data transmission becomes a challenging issue in wireless communication.

Wireless sensor networks benefit from the technical support brought by the rise of sensor technology, embedded computing technology, distributed information processing technology, and wireless communication technology, combining features such as high sensing, computing and communication capabilities, low cost, low power consumption, multifunctionality, small size, and short-range wireless communication, making it of interest to various industries [3]. Although traditional social network applications using cloud computing platforms to place user data can provide better storage services for massive amounts of user data, cloud data centers are generally far away from users, and it is difficult to ensure that users are more comfortable with all types of new social media in real-time requirements. The flexibility, fault tolerance, and rapid deployment of sensor networks make it widely used in environmental, food, and industrial fields, and it is considered one of the most important technologies of the twenty-first century. The ten emerging technologies with the most far-reaching impact in the future and wireless sensor networks are in the first place. The pervasiveness of wireless sensor networks determines its broad application prospects, and it can be evaluated as the most important technology in the twenty-first century, which is enough to represent its huge potential. A wireless sensor network by many inexpensive sensors randomly installed in the area to be observed, in the form of a multihop self-organizing network system, with only a small cost to the complex monitoring area for real-time monitoring, mastering the regional environment of each attribute data. Wireless sensor networks become a medium for indirect connection between users and the objective world, extending the way people and nature interact.

Wireless sensor network (WSN) reliability is the premise to ensure the normal operation of the network and is the basis for improving the performance of the network. WSN reliability not only is a key indicator of the network design but also ensures the normal operation of the network and management and maintenance of an important basis [4]. In the WSN, the sensor individual computing power, storage resources, and battery capacity are limited; sensor communication line bandwidth is limited, the transmission rate is low, there is mutual interference between signals, and transmission signal with the communication distance is constantly reduced; sensors are vulnerable to adverse weather, electromagnetic radiation, and other environmental factors; WSN is vulnerable to passive eavesdropping, active intrusion, denial of service, and other network attacks from the Internet [5]. For WSN reliability, research focuses on the difficulty of research in today's academic community and still has not formed a complete and more mature theoretical framework. Therefore, this study has important theoretical and practical value.

2. Related Works

Many types of research have been done to address the wireless sensor network reliability issues, such as proposing a

method based on automatic fault tree generation from the perspective of analyzing sensor failures to evaluate the reliability and availability of wireless sensor networks when failures occur on network devices. A reliability assessment method based on a hierarchical confidence rule base is proposed to analyze WSN reliability assessment from both internal faults and external attacks [6]. A detection method based on time series data of sensor networks is proposed to determine the source of faults using calculating the degree of difference between the test data and the normal interval. Object-oriented colored Petri nets are used as a modeling tool for heterogeneous wireless sensor networks, and a new quantitative method for the reliability assessment of heterogeneous wireless sensor networks is proposed. The above method has good analysis results for sensor failures, i.e., when the data changes drastically; however, satisfactory results cannot be achieved for insignificant data fluctuations.

According to research on WSN-based communication networks, the reliability of WSNs is mainly studied in terms of routing problems, reliable transmission problems, and network connectivity problems. A reliable method for evaluating WSNs in a malware environment is considered to guarantee the effectiveness of WSN data transmission. After comparing the reliability and performance of different routing algorithms for WSNs, a dynamic routing algorithm is proposed to achieve end-to-end reliable transmission. The problem of data reliability in event-driven WSNs is investigated [7]. Considering network connectivity, an uncertainty random spectrum is established to evaluate the survivability of mobile WSN. To meet the user's needs for WSN transmission reliability assessment, a task-oriented transmission path-based WSN transmission reliability assessment model is proposed. To address the inefficiency of transmitting multimedia data over WSNs, the WSN packet congestion control protocol is modified and a lightweight reliability mechanism is proposed. A reliability-improving cooperative communication data collection scheme is designed to achieve improved network communication reliability without degrading the network survival cycle.

One of the major characteristics of nodes in wireless sensor networks is that they have limited energy, and in the process of practical applications, the nodes are centrally powered by batteries. From the existing research, the early research on wireless sensor networks mainly focused on energy saving, that is, to ensure the normal and stable operation of wireless sensor networks by extending the life cycle of the network as much as possible by practical means [8]. The sharing and openness of wireless communication channels cannot meet the service requests of many users at the same time, resulting in lower communication quality and increasing the complexity of wireless transmission. At the same time, secure data transmission in wireless communication has become a challenging issue. However, the operational characteristics of the wireless sensor network itself can easily reduce the reliability of its transmission, so it is necessary to ensure the reliability of its transmission under the premise of energy saving. When applied to the monitoring of hazardous sources, because the node energy is limited and the node deployment location is not easy to replace the

battery, so it is necessary to ensure the balance of net energy during the monitoring process. In addition, it is necessary to avoid excessive use of a node prematurely exhausting energy and affecting data transmission. [9]. The birth of emerging technologies is usually associated with the context of a particular era, and the same is true for wireless sensor network technology. Today, many fields are in dire need of new technologies to help them evolve rapidly and achieve higher efficiency with as few human and material resources as possible. And many frontier fields of technology are usually closely related to IoT, and many research topics related to IoT have emerged, such as smart bracelets, smart homes, smart hotels, smart transportation, and smart manufacturing [10]. Not only that, wireless sensor network technology plays an extremely important role in diverse fields such as environmental monitoring, emergency rescue, natural disaster warning, and industrial and agricultural automation.

3. Wireless Sensor Social Network Data Transmission Reliability Model Design

3.1. Reliability Transmission Techniques. For the data forwarding process, not only the forwarding efficiency but also the stability needs to be considered. To ensure that data is received by the destination node stably and reliably, the trust degree among nodes needs to be considered when selecting relay nodes. Generally, the more frequent nodes with similar interests interact with each other, indicating a high trust degree and a more intimate relationship between them; therefore, the trust degree is crucial to the reliability of data forwarding [11]. To accurately quantify trustworthiness, this paper uses similarity and interaction degrees, which reflect the similar interests and frequency of interactions between nodes, respectively. To accurately measure the similarity between nodes, common neighbor nodes are used as the same or similar interest of two nodes; the main reason is that the more common neighbor nodes of two nodes, the closer they are in the network, which can ensure the reliability of data forwarding. The similarity sim is used to denote the proportion of the number of common neighbor nodes of two nodes i and j , in which, to ensure transmission efficiency, then the selected node should have better forwarding ability than the carrying node, which means the influence degree of node j should be greater than that of node i . Secondly, to ensure the stability and reliability of data forwarding, then the selected node has a strong enough relationship with the carrying node, which means the trust degree of node j and node i should be greater than the average trust degree of node i and its neighbors; in addition, node j of the destination node relationship is better than that of the carrying node, which means that the trust between node j and destination node D is greater than the trust between node i and destination node D , as shown in the following equation:

$$sim_{ij} = \frac{1}{\sqrt{d_i + d_j}}. \quad (1)$$

Task reliability is defined as “the ability of a product to

perform a specified function within a specified task profile.” The definition of task reliability shows that task reliability is determined by the prescribed task profile; i.e., task reliability is related to the rules for determining task success or failure, the task time, and the stress conditions experienced by the product in chronological order during the task period and the environmental conditions, and task reliability reflects the success of the product in completing the task [12]. Therefore, when assessing mission reliability, it is only necessary to count the failures that occur during the mission period that jeopardize mission success. When judged from a “maintenance” perspective, any event or condition that causes a product to be repaired is considered a failure. This is the criterion for identifying faults that correspond to basic reliability. Such a failure may or may not affect the completion of the product’s task. If considered from the point of view of “mission accomplishment,” only the state or event that affects mission accomplishment is considered a fault or a fatal fault. This is the criterion for fault discrimination that corresponds to task reliability. The scope of failure in the former is greater than and includes the latter. Task profile means “A chronological description of the events and environment experienced by a product during the time it takes to complete a defined task.” One or more task profiles should be developed for each product that accomplishes one or more tasks. The task profiles include the elements shown in Figure 1.

This chapter considers a large-scale high-conflict WSN environment, which consists of hundreds of sensor nodes that are divided into different levels of clusters from high to low by a hierarchical clustering algorithm, where the nodes within each cluster send the sensed data information to a cluster head node generated through an election, and finally, the cluster head node forwards the collected data information of all the nodes within the cluster to the aggregation node through a multihop nodes. Different clusters can cause conflicts in the process of data transmission, resulting in the loss of data information, and the failure of the node responsible for forwarding can also cause the loss of data information. To facilitate the study, it is agreed that the WSN network model has the following properties.

- (1) High-density characteristics, with no isolated nodes under initial conditions
- (2) The base station is unique and has no energy limitations
- (3) The initial energy of the sensor nodes is all, and the energy cannot be increased
- (4) Sensor nodes have some data fusion capability and are uniquely identified
- (5) Sensor nodes have localization capability

The structural model diagram of the network is shown below, the sensor node sends the sensed data information to the cluster head node of that cluster, the cluster head divides the packet into several subpackets based on the local routing table information and transmits the subpackets to

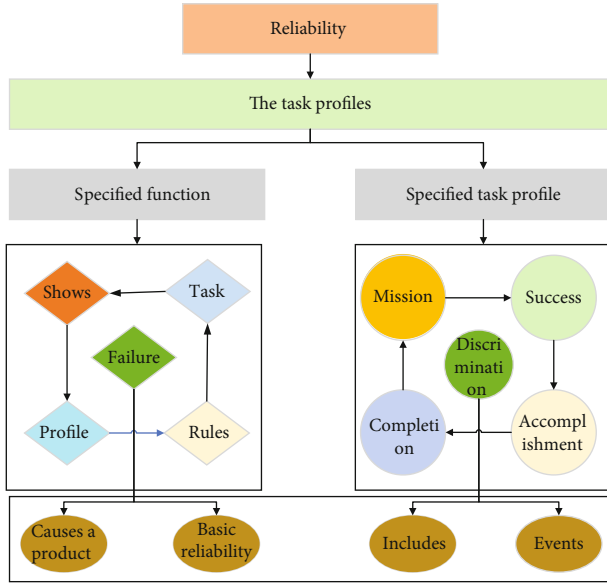


FIGURE 1: Contents of the mission profile.

the aggregation node through the intermediate node in a concurrent multipath manner, the aggregation node receives the subpackets from the same cluster and performs a simple data fusion, and if it forms the complete original packet, then all the subpackets of that cluster on the transmission line are automatically dropped, as shown in Figure 2.

The fault diagnosis of WSN contains two parts of work, fault detection and fault type judgment, for the workflow of the fault diagnosis model [13]. In fault detection, the sensor data is analyzed to find the abnormal data present; in fault type judgment, the prerequisite attributes of sensor data are extracted and the fault type of sensor data is found through a hierarchical BRB model. In WSN when a sensor node fails, it generates a large amount of abnormal data that deviates from the normal value, and the comparison of normal and abnormal data can achieve fault detection in WSN. The flexibility, fault tolerance, and rapid deployment of sensor networks make it widely used in the environment, food, industry, and other fields. It is considered one of the most important technologies in the 21st century. Among the ten emerging technologies with the most far-reaching impact in the future, wireless sensor networks rank first. The universality of wireless sensor networks determines its broad application prospects, and it can be evaluated as the most important technology in the 21st century, which is enough to represent its huge potential. To achieve reasonable fault detection requires clustering analysis of sensor nodes, similarity comparison of data between sensor nodes within a cluster, and when the cumulative deviation of sensor data exceeds the reservation threshold within a certain time, the current sensor node is possibly faulty. Through fault detection, WSN abnormal data is found and it is difficult to discover the fault type directly from the sensor data when the fault type is determined, so the data is characterized. The prerequisite attributes of the data can be extracted by data correlation features, including temporal correlation, spatial correlation, and attribute correlation. A hierarchical BRB

model structure is proposed on how to reasonably utilize these prerequisite attributes to construct a BRB model while solving the rule explosion problem of the BRB model due to too many prerequisite attributes and improving the detection accuracy of the BRB model. The basic structure of the layered BRB system uses the output results of the current layer of BRB as the input of the next layer of BRB models, thus realizing the conversion of a complex BRB model into multiple simple BRB models.

$$\frac{A_I^{i-1} - a_i^{(t)}}{A_i^i - A_I^{i-1}} = l. \quad (2)$$

Wireless sensor networks can provide versatile applications and great benefits for smart cities and intelligent transportation systems. There are various types of services and applications in wireless sensor networks, such as real-time traffic monitoring, security information exchange, and seismic activity monitoring. Open wireless networks, social networks, and smart grids allow other users to easily join the system. This sharing model makes these wireless networks vulnerable to various attacks, converting them to internal attackers in case the attacker captures them internally and affects the normal operation of the network. Our approach develops availability weights based on statistical representations of internal malicious nodes and incorporates them into optimization problems that can be widely used in many practical scenarios [14].

During the work of wireless sensor networks, affected by various factors, the data collected by the sensor nodes may be different from the real environmental information and inevitably interspersed with noise. For this phenomenon, it is assumed that the reliability changes of sensor nodes due to different factors are expressed through the uncertainty of monitoring data, such network blockage will cause some node data loss, and node energy deficiency will cause data distortion. Therefore, this paper analyzes the node data reliability from the perspective of monitoring data changes. Combined with the data reliability assessment model of wireless sensor networks based on evidence-based inference rules, the possible problems in practical engineering are summarized as follows: Problem 1—WSN data reliability assessment index construction problem. In this paper, the reliability of wireless sensor networks is mainly assessed by analyzing the monitoring data of wireless sensor networks, and it is especially important to construct reasonable and credible assessment indicators. The following indicator system model is established.

$$S = (x_1, x_2, \dots, x_n), \quad (3)$$

where S denotes the indicator system, x_i denotes the i th indicator, and I denotes the number of indicators.

3.2. Data Transmission Reliability Model Design for Wireless Sensor Social Networks. The basic structure of the data reliability assessment model for wireless sensor networks considering perturbation is based on evidence-based inference

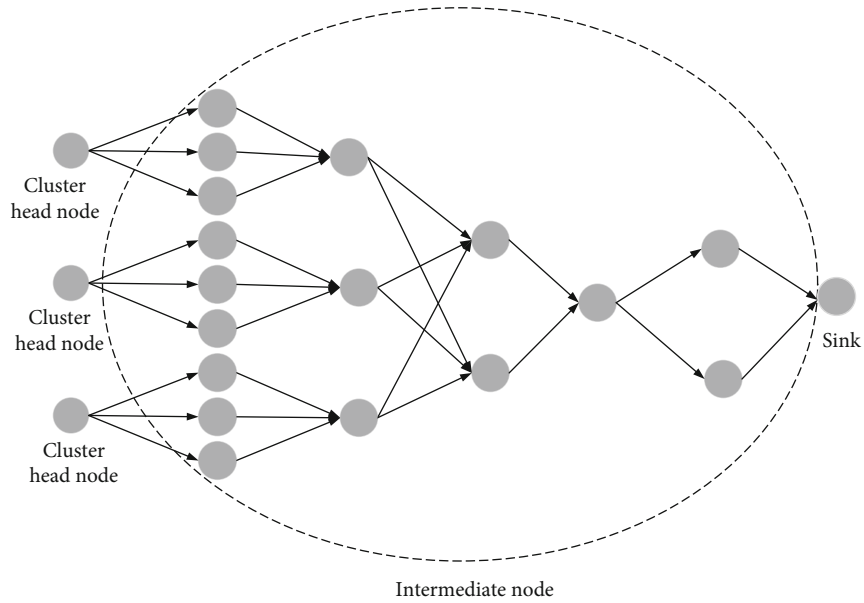


FIGURE 2: Model diagram of a packet structure.

rules with the model mentioned in Section 3.1. Firstly, the assessment index system is constructed, and the index data are unified by a rule-based approach to identify the framework; after that, the weights and reliability of the index data are calculated, and the data reliability is assessed by evidence-based inference rules, compared with the aforementioned model, the assessment considering perturbation. The model also requires a random variation of the data to simulate the impact of the perturbed environment on the sensor data, and the impact of the perturbation on the original data is analyzed by calculating the perturbation factor and setting the maximum perturbation error to indicate the adaptability of the sensor to that perturbed environment. The data reliability assessment method of sensor node based on evidence inference rule in the perturbed environment uses ER rule to fuse the information of indicator data and parameters based on the standardization of indicator data as well as its weight and reliability and calculates the data reliability of sensor node at a certain moment, and the following will analyze the implementation process of ER rule in detail for the calculation formula of ER rule. Suppose a node collects a total of T data, each information contains I indicators, and the evidence after data normalization can be expressed as the following confidence distribution form.

$$e_i = \{(H_n, P_j), n = 1, j = -1\}. \quad (4)$$

After analyzing the sensor node data reliability by ER rules, the real-time state of sensor node reliability can be observed, but the perturbation of the sensor node by external factors is not considered; however, the analysis of the sensor operating mode reveals that it is inevitably disturbed by various factors. In this subsection, based on the above-proposed sensor node data reliability assessment model considering perturbations, the nodes are evaluated for reliability to sim-

ulate the operating state of the nodes affected by different factors by adding perturbation variables to the nominal trajectory and setting perturbations of different strengths, with the perturbation variables representing the actual data of the sensor nodes relative to the perceived information in the unperturbed environment. Two laws are met: the generation of perturbations is random and irregular, and the generation of perturbation variables conforms to the characteristics of normal distribution. Analyzing the perturbation factors affecting the index data, the accuracy of temperature data is easily affected by network fluctuations and environmental confrontation. In this paper, we simulate four types of perturbed environments (weak network fluctuations and weak environmental confrontation, weak network fluctuations and strong environmental confrontation, strong network fluctuations and weak environmental confrontation, strong network fluctuations, and strong environmental confrontation), and the corresponding perturbation strengths are 0.015, 0.030, 0.045, and 0.060, respectively. After adding the perturbation, the data of each indicator changes, as shown in Figure 3.

However, data transmission is not guaranteed immediately after the nodes meet, because the resource-limited channel may be busy and the nodes can use the channel to complete data forwarding only when the channel becomes idle. Therefore, the idle waiting time of the channel after two nodes meet until they start transmitting data needs to be analyzed. Different from the general waiting rule, this paper uses the channel in the order of the priority of the nodes' influence, which is because the nodes with higher influence have a higher probability of carrying high-value data, which can make the channel resources more efficient. During data transmission, the channel will show two states: first, the channel is idle, when node i sends data directly to node j ; second, the channel is busy, when node i needs to wait for the channel to become idle before competing with

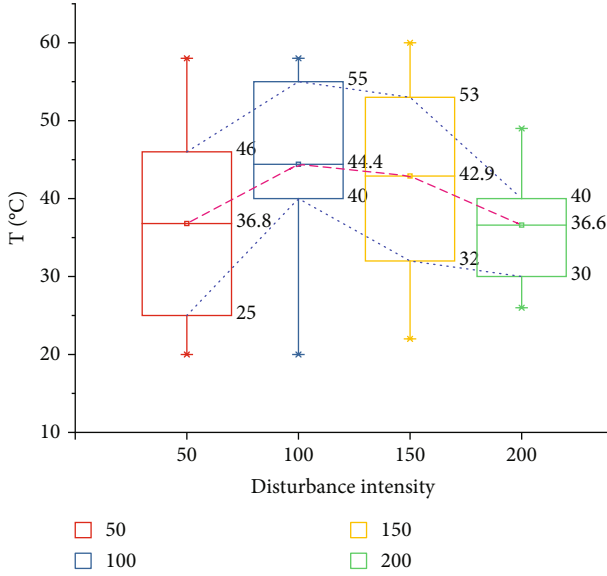


FIGURE 3: Temperature data corresponding to the intensity of the disturbance.

other nodes for the channel. Therefore, there are two issues to consider: whether the channel is busy or not and the waiting time when the channel is busy [15]. In general, whether the channel is busy or not is related to two factors, namely, the channel bandwidth and the number of nodes competing for the channel, which are exponentially related to the probability of the channel being busy, because channel competition decreases significantly with each doubling of the bandwidth at low bandwidths, while the number of nodes competing for the channel is the opposite.

$$R(t) = \sum_{u=t}^{N_y} L(I_t : I_u) + 1. \quad (5)$$

When a cluster head node fails, if there is no other redundant node for continued transmission, then, the data of that node may be lost and will reduce the reliability of the network. If a normal node reselects another cluster head node for data delivery, it is not only a complex process for the nodes in the failed cluster, but it is also a nontrivial task for the clusters that wish to join to deal with the newly joined nodes. For example, cluster head nodes (routers) and sink nodes (coordinators) take the backup redundancy of cluster head nodes so that the overall reliability of the cluster head nodes is the best, thus improving the reliability of the whole monitoring system. At this point, when a cluster head fails, it is no longer considered a single failed body, but as a group of 1 cluster head node. When an individual node in the node group fails, a redundancy mechanism is used, and another link can be selected for the transmission of information, ensuring the connectivity of the communication link. When a cluster head node fails, another backup cluster head node takes over the work, which not only reduces the overhead of route finding but also reduces the complexity of controlling other cluster head nodes [16].

Assuming that the number of redundancies of cluster head nodes is $k = 1, 2, 3, \dots, 10$, the relationship between cluster head node reliability and the number of redundancies is proportional, the more the number of redundancies, the higher the reliability of cluster head nodes will be, when the number of redundancies is 2, and the reliability of cluster head nodes is significantly improved, when the number of redundancies reaches 3. However, it is not better to have more redundancy because the actual deployment needs to consider the budget, and the cluster head nodes are more expensive. When the number of redundancies reaches 3 or more, the reliability of the cluster head is almost the same and does not improve significantly, as shown in Figure 4.

We assume that the source node has no prior knowledge of the abnormal behavior of the node that is working. We do not assume the policies, targets of failure behavior, or movement patterns of malicious nodes. We assume that the type of misbehavior, such as internal component failure or external failure, is not known in the network. To characterize the impact of node misbehavior on multiple types of transmissions, each source must collect information about the impact of misbehavior in the urban network. When sensor node I provides multiple types of services to the receiving node through multihop communication, there exist some candidate forwarding nodes based on node i 's knowledge of the available neighbors. Each sensor node tries to maximize its revenue by sending feedback signals, and the "resource price" determines the cost of consuming these limited resources for the competing services. Therefore, each node charges a resource price and then allocates a certain number of resources to be made available to users. For various types of services or applications, each source is associated with a utility function that reflects how much of a quality of service (QoS) benefit the source receives as measured by the allocated transmission rate. Here, the network model in a distributed framework for candidate node selection and rate allocation of sources is shown in Figure 5.

4. Wireless Sensor Network Topology Reliability Assessment

4.1. Reliability Assessment. The network may be affected by various factors such as component failure, traffic changes, and routing methods; during the operation, the complexity and randomness of the network present a great challenge to network reliability analysis, and it is difficult to establish an analytical model for network reliability assessment; therefore, many researchers use simulation or statistical approach to analyze the network reliability [17]. The simulation method is the main way of current and even future network reliability assessment, by constructing a network reliability model, setting up a model of random parameters in the network such as tasks, failures, and maintenance, simulating the state changes in the network, and then statistically analyzing the corresponding reliability parameters. At present, there exist two main types of simulation methods: Monte Carlo and state machine. The Monte Carlo method is a probabilistic statistical method to obtain results by random sampling. Based on the results of the analysis of the actual problem,

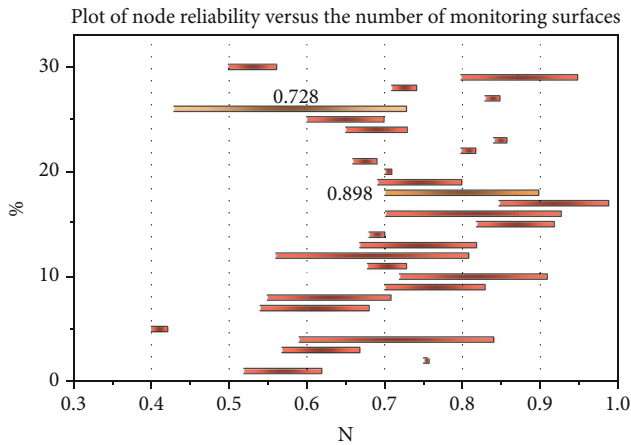


FIGURE 4: Plot of node reliability versus the number of monitoring surfaces.

random events are constructed to describe the probabilistic process, and the solution of the problem is obtained by sampling and calculating the random events. The process of constructing a reliability evaluation model of a network based on network topology, network protocols, and business processes by simulating the current common network performance simulation tools such as OPNET, NS2, and OMNESE is a Monte Carlo method.

$$N_e = \begin{cases} \frac{w}{r} > \frac{\sqrt{5}r}{2}, \\ \frac{w}{2r} \leq \frac{\sqrt{5}r}{2}. \end{cases} \quad (6)$$

Input random parameters such as network traffic and fault distribution are sampled and calculated to obtain the relevant reliability parameters. For complex discrete events in networks, state machines are used to describe network changes and analyze the transfer process of network states to assess network reliability. Among the state machine-based modeling approaches, Petri nets, which simulate discrete-event dynamic systems, are commonly used modeling tools. Petri nets can depict multiple logical relationships and events in the system such as resource sharing, competition, and conflict in synchronous as well as asynchronous. However, when modeling large-scale complex network systems, general Petri nets are prone to the “state combination explosion” phenomenon. To address this problem, researchers have proposed various advanced models of Petri nets such as Coloring Petri Nets (CPN), Stochastic Petri Nets (SPN), and Object-Oriented Petr Nets for modeling. Aiming at the problem of low efficiency in transmitting multimedia data on WSN, the WSN data packet congestion control protocol was modified, and a lightweight reliability mechanism was proposed. A scheme of collaborative communication data collection with improved reliability is designed, which can improve the reliability of network communication without reducing the network life cycle. Redundancy is usually used in wireless sensor networks to improve

reliability; however, energy saving and high reliability are two conflicting goals, so it becomes a challenge to integrate high reliability and low energy consumption for transmission task assignment in wireless sensor networks [18]. The goal of this chapter is to minimize the energy consumption of transmission task assignment in wireless sensor networks with the deadline of the task and the reliability of the task as a constraint.

To achieve this goal, a centralized reliable and efficient transmission task assignment strategy for wireless sensor networks is proposed, in which the task is taken as the malfactor object and the transmission task assignment process is executed by the sink node after the required network information is collected; based on the global network state information, the wireless sensor network transmission task assignment problem is transformed into a nonlinear mixed-integer programming problem. Many researchers have researched the transmission task allocation problem of wireless sensor networks. Since WSN nodes are resource-constrained, one of the main objectives of task assignment in this environment is to minimize energy consumption and thus maximize the system operational lifetime. Therefore, the objective of traditional wireless sensor network transmission task allocation is mainly focused on energy saving. Among the methods for solving the task assignment problem, the exact solution methods such as integer programming, branch-and-bound method, and enumeration method cannot meet the real-time requirements; while the dynamic planning-based heuristics are more efficient to solve, but they all use a local search strategy based on greedy strategy, so the obtained task assignment scheme may not be the optimal one, as shown in Figure 6.

In this paper, the message retransmission technique is used in the backbone transmission part to ensure reliable data transmission. A scheme is proposed for message delivery using hop-by-hop broadcasting and copying multiple copies of the same message with improved reliability, using wireless broadcasting to increase the packet delivery rate per-hop and to obtain the required reliability at minimum cost, and finally deriving the optimal policy used to distribute the required reliability at each hop point to obtain the required end-to-end reliability for any given. This approach can reduce the probability of packet loss, but because replicating multiple copies and sending them entails significant energy consumption, especially in large networks. To avoid duplication of messages, a new decentralized technique called Geographic Forwarding Rules (GFRs) is proposed to reduce the number of broadcast messages in mobile self-organizing networks by dividing the network into virtual regions using the location information of the nodes and avoiding duplication of messages between regions.

4.2. Simulation Verification and Analysis of Results. To be able to clearly illustrate the factors influencing the transmission capacity and to verify the accuracy of the proposed analysis process, an empirical dataset was used, which was completed by 100 volunteers during the INFOCOM06 conference, each of whom carried a mobile terminal with a Bluetooth interface and the trajectories of these volunteers and

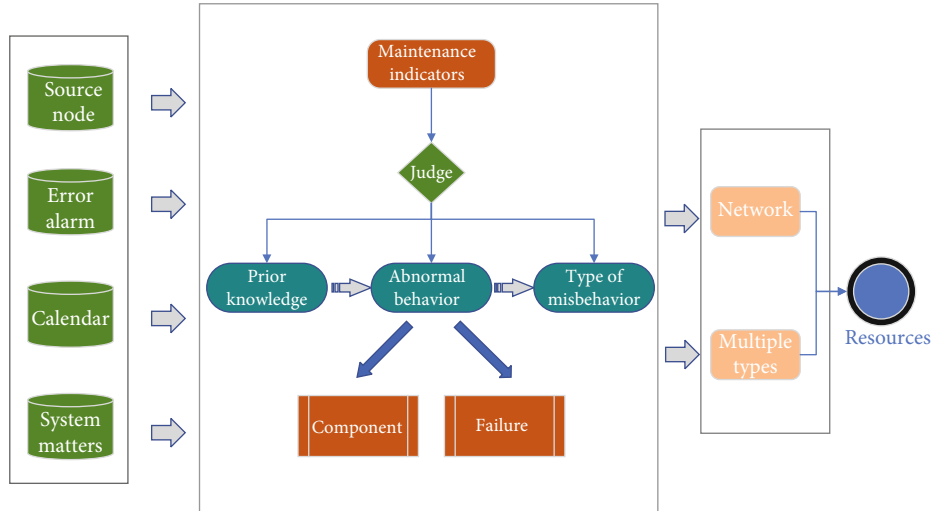


FIGURE 5: Multiservice transfer framework for fault activity information.

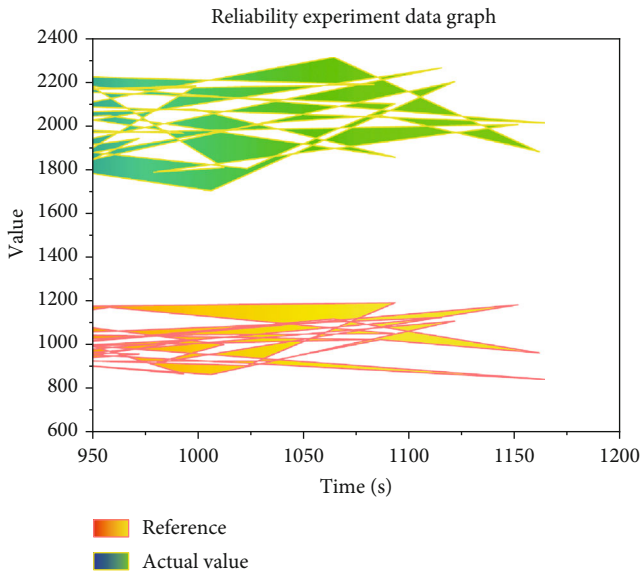


FIGURE 6: Reliability experiment data graph.

the contact records, which can reflect the mobile characteristics of the nodes and their social relationships. The dataset is used by several laboratories at home and abroad and has high authority [19]. In this paper, we use the MATLAB simulation platform to compare and analyze the difference between the theoretical numerical results and simulation numerical results, and the THR and SML appearing in the later figures indicate the theoretical results and simulation results, respectively. The operating characteristics of the wireless sensor network itself can easily reduce the reliability of its own transmission, so on the premise of ensuring energy saving, it is also necessary to ensure the reliability of its transmission. When applied to the monitoring of hazardous sources, because the energy of the node is limited and the location of the node is not easy to replace the battery, it is necessary to ensure that the network energy is balanced dur-

ing the monitoring process, affecting the transmission of data. In this section, we analyze the relationship between the transmission capacity S and the number of network nodes N , the number of hops H , the packet loss rate P , and the delay T , respectively, and also analyze the relationship between the packet loss rate and the delay to better understand the trend between these variables. The simulation parameters are set as shown in Table 1.

According to the small world theory, any two nodes in the network can communicate with the help of a limited number of nodes, and the number of these collaborating nodes is generally 2-6, so this section first analyzes the effect of the number of network nodes N on the transmission capacity S at different hop counts ($H = 2, H = 4, H = 6$). From the results, it can be found that the transmission capacity increases with the increase in the number of network nodes at different hop counts, but the overall transmission capacity under 4 hops is higher than under 2 and 6 hops; this is because the data has the best transmission performance only when the number of hops is within a certain range; too high or too low is not good for data forwarding. In addition, as the number of nodes increases, the transmission capacity grows faster under 4 hops. Two-hop transmission capacity increases slowly and decreases to a certain extent when $N \geq 120$. This is because the network nodes increase to a certain level and fewer relay nodes make the total time required to transmit data grow, resulting in a decrease in transmission capacity. Finally, the numerical results of the simulation and theoretical analysis match with an average error of 12%.

$$\lambda_{u_{ij}} = W_{u_{ij}/d_{u_1}} \cdot \quad (7)$$

Keeping the communication distance constant and increasing the number of nodes within the network, we can see that the traditional chance routing algorithm starts to have node failures about 1 minute into the simulation, relying solely on the geographic location information of

TABLE 1: Simulation parameter settings.

Simulation parameters	Reference	Actual value
Number of nodes	80-150	120
Communication module	Bluetooth	ZigBee
Network area	1000,1000	1000,1000
Subchannel rate	100	103
Node cache space	20-50	30

neighboring nodes and sink nodes to determine intermediate forwarding nodes [20]. In this case, it is considered that the closer the sink node within the transmission range, the better the path. This will result in the frequent use of a node as an intermediate node for data forwarding during the initial process of the network until the node fails with energy exhaustion, while many nodes will have energy redundancy and the energy will not be utilized after the overall failure of the network. With the improved chance routing algorithm, the network energy consumption can be evenly distributed to neighboring nodes, which increases the network survival time until the surrounding nodes are depleted of energy before they fail centrally at 14 minutes, basically reaching the maximum network survival time, as shown in Figure 7.

Due to the backbone role of the cluster head node in the network, in this paper, the cluster head node is evaluated as a separate component and both upstream and downstream transmission processes are divided into two phases using the cluster head node as the boundary and modeled in a stepwise manner to facilitate the application and extension of the reliability assessment model. Wireless sensor networks have complementary and redundant relationships in space and time between the information sent out by multiple sources when monitoring the same event or parameter. Many source nodes in a cluster topology send sensing information to the cluster head node, which determines whether the sensing task is completed based on comparison with a threshold value. In the uplink transmission phase of mesh-type (mesh) topology, multiple source nodes transmit the sensed information to the sink node, so this phase is a multisource single-homed network. For the same task in a multisource environment, it is not required that every packet sensed by each source node be successfully received by the sink node. Unlike the cluster topology where the sensed packets are prone to data fusion at the cluster head, the mesh topology is less efficient in performing data fusion at the intermediate nodes of the network. For modeling, it is assumed that the data sensed by the source nodes in the mesh-type topology is not subjected to data fusion. To accurately measure the similarity between nodes, the common neighbor node is regarded as the same or similar interest of two nodes. The main reason is that the more common the neighbor nodes of two nodes, the closer their relationship in the network can ensure data forwarding. The similarity sim_{ij} is used to represent the proportion of the number of common neighbor nodes of two nodes i and j .

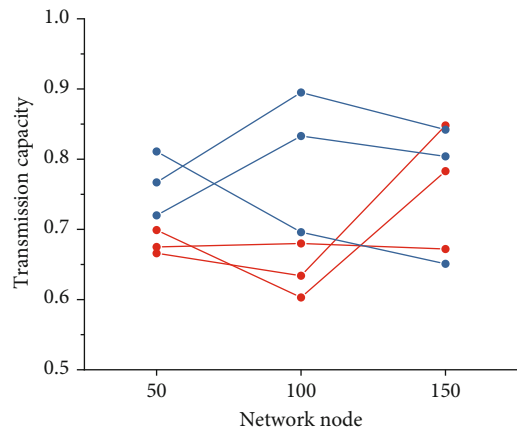


FIGURE 7: Transmission capacity versus network nodes.

5. Conclusion

The reliability of wireless sensor networks (WSNs) is one of the important indicators of network quality of service and requires system planning and a series of designs and verification to achieve reliability goals. Existing studies have mainly investigated the basic reliability of the network in terms of the connectivity of the network, the capacity of the network, and individual performance parameters such as delay and packet loss. However, these parameters are difficult to assess the comprehensive capability of the network when running services, which requires an overall evaluation and design of the mission reliability of the network. Task reliability is closely related to the task profile, functional requirements, state mode, and system configuration of the network; as the WSN continues to expand, the association relationships between nodes within the network become more complex and the system operation states increase, leading to increased difficulty in the analysis and design process of WSN task reliability. Task reliability is a comprehensive reflection of various characteristics of the network; therefore, the analysis and design of task reliability of WSNs are a difficult point that needs to be broken. In this paper, the hierarchical clustering protocol is designed from the perspective of saving energy consumption of WSN, and the reliable data transmission protocol is designed to ensure reliable data transmission, but the idea is not perfect, and there are still many topics to be improved or to be studied in the field of WSN.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The study was supported by the Construction of First-Class Disciplines in Ningxia Colleges and Universities (Pedagogy) (Grant No. NXYLXK2017B11).

References

- [1] Y. Liu, D. Liu, Y. Zhao, and L. Wang, "The reliability analysis of wireless sensor networks based on the energy restrictions," *International Journal of Wireless and Mobile Computing*, vol. 10, no. 4, pp. 399–406, 2016.
- [2] L. Xing, "Reliability modeling of wireless sensor networks: a review," *Recent Patents on Engineering*, vol. 15, no. 1, pp. 3–11, 2021.
- [3] Z. Zou and Y. Qian, "Wireless sensor network routing method based on improved ant colony algorithm," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 3, pp. 991–998, 2019.
- [4] M. Abdulkarem, K. Samsudin, F. Z. Rokhani, and M. F. A. Rasid, "Wireless sensor network for structural health monitoring: a contemporary review of technologies, challenges, and future direction," *Structural Health Monitoring*, vol. 19, no. 3, pp. 693–735, 2020.
- [5] W. Zhang, S. Zhu, J. Tang, and N. Xiong, "A novel trust management scheme based on Dempster–Shafer evidence theory for malicious nodes detection in wireless sensor networks," *The Journal of Supercomputing*, vol. 74, no. 4, pp. 1779–1801, 2018.
- [6] Q. Huamei, J. Tao, J. Su, Z. Zhiwen, and X. Wangping, "QoS adaptive and energy aware cross-layer opportunistic routing protocol in wireless sensor networks," *IET Communications*, vol. 13, no. 8, pp. 1034–1042, 2019.
- [7] V. Gaur, O. P. Yadav, G. Soni, and A. P. S. Rathore, "A literature review on network reliability analysis and its engineering applications," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 235, no. 2, pp. 167–181, 2021.
- [8] S. Tamilselvi and S. Rizwana, "Optimized cluster head selection with traffic-aware reliability enhanced routing protocol for heterogeneous wireless sensor network (HWSN)," *International Journal of Computer Networks and Applications*, vol. 8, no. 2, pp. 108–118, 2021.
- [9] L. Chan, K. Gomez Chavez, H. Rudolph, and A. Hourani, "Hierarchical routing protocols for wireless sensor network: a compressive survey," *Wireless Networks*, vol. 26, no. 5, pp. 3291–3314, 2020.
- [10] T. A. Alghamdi, "Energy efficient protocol in wireless sensor network: optimized cluster head selection model," *Telecommunication Systems*, vol. 74, no. 3, pp. 331–345, 2020.
- [11] G. Khanna, S. K. Chaturvedi, and S. Soh, "Two-terminal reliability analysis for time-evolving and predictable delay-tolerant networks," *Recent Advances in Electrical & Electronic Engineering (Formerly Recent Patents on Electrical & Electronic Engineering)*, vol. 13, no. 2, pp. 236–250, 2020.
- [12] S. Din, A. Paul, A. Ahmad, and J. H. Kim, "Energy efficient topology management scheme based on clustering technique for software defined wireless sensor network," *Peer-to-Peer Networking and Applications*, vol. 12, no. 2, pp. 348–356, 2019.
- [13] Nizirwan Anwar, Dewanto Rosian Adhy, Budi Tjahjono, Rudi Hermawan, Nur Widiyasono, and Muhammad Abdullah Hadi, "Reliability analysis of communication network service quality for internet of vehicles (IoV)," *International Journal of Science, Technology & Management*, vol. 2, no. 5, pp. 1588–1599, 2021.
- [14] R. P. Ojha, P. K. Srivastava, G. Sanyal, and N. Gupta, "Improved model for the stability analysis of wireless sensor network against malware attacks," *Wireless Personal Communications*, vol. 116, no. 3, pp. 2525–2548, 2021.
- [15] M. Mathapati, T. S. Kumaran, A. Muruganandham, and M. Mathivanan, "Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 6, pp. 6047–6055, 2021.
- [16] D. J. I. Zong Chen and K. L. Lai, "Machine learning based energy management at Internet of Things network nodes," *Journal: Journal of Trends in Computer Science and Smart Technology September*, vol. 2, no. 3, pp. 127–133, 2020.
- [17] D. Hosahalli and K. G. Srinivas, "Enhanced reinforcement learning assisted dynamic power management model for Internet-of-things centric wireless sensor network," *IET Communications*, vol. 14, no. 21, pp. 3748–3760, 2020.
- [18] M. Abdelhafidh, M. Fourati, L. C. Fourati, and A. Chouaya, "Wireless sensor network monitoring system: architecture, applications and future directions," *International Journal of Communication Networks and Distributed Systems*, vol. 23, no. 4, pp. 413–451, 2019.
- [19] P. Joshi and A. S. Raghuvanshi, "Hybrid approaches to address various challenges in wireless sensor network for IoT applications: opportunities and open problems," *International Journal of Computer Networks and Applications*, vol. 8, no. 3, pp. 151–187, 2021.
- [20] G. F. Albery, L. Kirkpatrick, J. A. Firth, and S. Bansal, "Unifying spatial and social network analysis in disease ecology," *Journal of Animal Ecology*, vol. 90, no. 1, pp. 45–61, 2021.