Hindawi
Journal of Sensors
Volume 2022, Article ID 3842722, 12 pages
https://doi.org/10.1155/2022/3842722

Research Article

Data Transmission Reliability Analysis of Wireless Sensor Networks for Social Network Optimization

Xia Xu,[1] **Jin Tang**,[1] **and Hua Xiang**[2]

[1]*School of Information Science, Changjiang Polytechnic, Wuhan, Hubei 430074, China*
[2]*School of Computer Science, Changjiang University, Jingzhou, Hubei 434023, China*

Correspondence should be addressed to Hua Xiang; xianghua@yangtzeu.edu.cn

Received 2 November 2021; Revised 6 December 2021; Accepted 7 December 2021; Published 6 January 2022

Academic Editor: Gengxin Sun

With the rapid development of the Internet in recent years, people are using the Internet less and less frequently. People publish and obtain information through various channels on the Internet, and online social networks have become one of the most important channels. Many nodes in social networks and frequent interactions between nodes create great difficulties for privacy protection, and some of the existing studies also have problems such as cumbersome computational steps and low efficiency. In this paper, we take the complex environment of social networks as the research background and focus on the key issues of mobile wireless sensor network reliability from the mobile wireless sensor networks that apply to large-scale, simpler information, and delay tolerance. By introducing intelligent learning methods and swarm intelligence bionic optimization algorithms, we address reliability issues such as mobile wireless sensor network fault prediction methods and topology reliability assessment methods in industrial application environments, the impact of mobile path optimization of mobile wireless sensor networks on data collection efficiency and network reliability, reliable data transmission based on data fusion methods, and intelligent fault tolerance strategies for multipath routing to ensure mobile wireless sensor networks operate energy-efficiently and reliably in complex industrial application environments.

1. Introduction

With the deep development of Internet technology and computer technology, the emergence of social networks has changed the traditional way of human socialization, and social networks have gradually become the main place for people's daily activities (entertainment and communication, online shopping, community Q&A, online education, etc.), and there are more and more participants in social networks, and information is spread in social networks at an unprecedented speed [1]. Through social networks, we can communicate in-depth with our friends in the form of sending messages, sharing content, etc. Due to its convenience and easy-to-use characteristics, social networks have become more and more common in people's lives and work under the environment of increasingly mature network technology. At the same time, with the rapid development of the network, the privacy issues therein are gradually attracting widespread attention. The wireless sensor network is an intelligent network that transmits data in the form of proximity multihop self-organization and collaboration and cooperation between nodes by deploying various types of sensor nodes to the monitoring area [2]. The network integrates information sensing, wireless communication, embedded computing, distributed information processing, and other technologies, the nodes preprocess the collected data and send it to the aggregation nodes in the form of multihop self-organization, and the aggregation nodes then transmit the collected information to the monitoring centre, which performs appropriate processing and finally feeds the processed data back to the decision-makers and transmits it to the required users. The physical links and capacities are mapped to traffic paths during the evaluation process, which can concisely reflect the performance degradation of the network. When evaluating the network performance reliability, the probability that the information from the source node reaches the destination node within the specified time is used as the timely reliability of this network,

the probability that the routing buffer overflows is used as the criterion to evaluate the network congestion, and the ratio of the packet received at the receiver side to the transmission at the sender side can also be used as the complete reliability of this network.

Privacy data in social networks mainly includes user's identity information, login information, friend information, the content published on the social network platform, and the dissemination of information. The root cause of privacy security risks in social networks is that the private data of data owners are distributed on social networking platforms without the direct physical control of data owners, which may cause data leakage and allow users who do not have access rights to view the content published by data owners or even users who maliciously steal information to view it. Studying how to combine data publishing methods with privacy-preserving techniques and prevent leakage of sensitive user information has become a serious challenge for current social networking services [3].

The reliability of WSNs (wireless sensor networks) is an important indicator for assessing network performance and can be classified into different categories based on different criteria. From the perspective of application requirements, dependability assessment can be divided into coverage-based and connectivity-based reliability; according to the different methods used for reliability analysis and calculation, reliability assessment can be divided into conditional probability, Markov chain, block diagram method, Monte Carlo simulation method, binary decision diagram, fault tree analysis, etc.; in addition, from the definition of division, it can be divided into task-based reliability and lifetime distribution-based reliability [4]. In this paper, we propose to carry out research on mobile wireless sensor network reliability problems and conduct an in-depth and systematic study in mobile wireless sensor network reliability assessment and optimization by introducing intelligent optimization algorithms and swarm intelligent bionic optimization methods, to address mobile wireless sensor network node hardware and network failure prediction methods, network reliability assessment methods for mesh, tree, and ribbon topologies, mobile path optimization on data collection efficiency and network reliability, reliable data transmission based on data fusion methods, and intelligent fault tolerance of multipath routing and other reliability issues, to provide an effective way to build a reliable mobile wireless sensor network suitable for the complex environment of social networks.

2. Related Work

The privacy and security of users in social networks is a pressing issue that is directly related to their safety in real life. Currently, researchers have carried out some research work on privacy metrics in social networks, but the research is still relatively lagging compared to industrial networks. The reliability of WSNs is mainly studied in terms of the failure problem of nodes and energy problem.

The problem of random failure of nodes is considered in the distributed WSN in the literature [5] for the analysis of the WSN feasibility. In the literature [6], a wireless sensor network consisting of a Sink node and n sensor nodes is considered and the reliability of the network is evaluated using probabilistic analysis. The concept of common cause failure is introduced in the literature [7], and a Monte Carlo simulation-based approach is proposed to calculate the reliability of the wireless sensor network. The Markov model is introduced in the literature [8] to evaluate the reliability of sensor nodes. A binary decision graph algorithm is proposed in the literature [9] to address the reliability of WSNs in a common cause failure environment. Common cause failure is defined as the phenomenon of simultaneous failure of multiple components in the network; for example, multiple sensor nodes in the network will fail simultaneously during an avalanche; previous WSN reliability analyses assume that sensor nodes are independent of each other and do not consider the effective correlation of sensor nodes; this analysis is not comprehensive; the literature [10] transforms the binary decision diagram into an ordered bifurcated decision diagram (OBDD) to consider the common cause events, which has been of great help to later scholars in their research. The literature [11] proposed the use of a survey questionnaire to count multiple metrics, through which users who may differ significantly in their privacy-preserving behaviours are selected to count their scores and then validate the validity of these metrics. In their study, they analyze the correlation between the scores of the survey metrics and two established privacy-preserving behaviours. Ultimately, they conclude that these metrics are a reliable and valid web management tool that can be used in research on online privacy metrics. In the literature [12], a dual objective function was constructed with the goal of shortest transport distance and highest security, and an adaptive random selection algorithm and a time adjustment algorithm were added to the ALNS heuristic to solve the transport path and improve the security of the transport path. The literature [13] combines the road class and road traffic influence factors in the actual dynamic road network and uses an improved ant colony algorithm to explore the optimal path that meets the requirements of travellers. The literature [14] proposes an algorithm to improve the reliability of paths between customers and target users in social networks, which uses a reverse ant colony algorithm with an improved pheromone update strategy in it, thus ensuring load balancing and shorter user waiting time. In the literature [15], path reachability, optimal path selection, and TOP-K path query are studied with graph data, and the objective and subjective weights of each attribute of the path are derived using information entropy technique and subjective assignment method for the case of mixing different types and characteristics of attributes such as deterministic and uncertainty in complex multiattributes, and then, the two weights are analyzed comprehensively to calculate each path's combined score and reduce the search space when optimizing the path query by graph decomposition and hierarchical shrinkage techniques. In terms of network routing, literature [16] proposed a general method to solve multiconstrained path queries by minimizing the nonlinear cost function to determine whether the found path is feasible and by minimizing

the main cost function to explore whether there are still better paths, thus ensuring QoS quality. The literature [17] proposes a difference-oriented path multiplex selection algorithm (CMT-DPS), where when the difference between paths is relatively large, paths of poorer quality are not selected to participate in data transmission, which improves the overall throughput and reduces the transmission delay to some extent. The software-defined network (SDN) path selection algorithm with dual impact factors based on the actual quality of experience (QoE) is proposed in the literature [18], which ensures link quality and load balancing by real-time state acquisition and dynamic adjustment of weights, while also applying the ant colony algorithm to improve the transmission rate.

3. Data Reliability Study of Wireless Sensor Networks for Social Network Optimization

3.1. Data Reliability Study of Wireless Sensor Networks. The basic reliability and mission reliability of a wireless network are the "one and two sides" of the product reliability work, "one" means that the main body of basic reliability and mission reliability implementation is the product design itself, "two sides 'one'" means that the main body of basic reliability and task reliability is the product design itself, and "two sides" means that basic reliability and task reliability are two objectives that should be taken into account in product design, and one is indispensable. From the definition of basic reliability and task reliability, we know that the difference between them is as follows: (1) The time definition is different. The scope of "specified time" in the definition of mission reliability is defined by the mission profile cycle. The "specified time" in the definition of basic reliability is defined by the full life cycle profile, which generally includes multiple task profiles. (2) The scope of failure statistics is different. When evaluating task reliability, only those failures that affect the "completion of the task" in the definition of task reliability are considered, and those failures that do not affect the completion of the task are not considered. However, when evaluating basic reliability, it is necessary to consider all the failures that need to be repaired during the whole system life cycle, and the scope of failures in basic reliability statistics is larger than that of mission reliability. (3) The final impact on product use is different. Basic reliability is related to maintenance coverage, and basic reliability ultimately affects the availability of equipment and the cost of maintenance coverage [19]. The continuous type of Weibull distribution and other distributions is closely related, and the range of values of shape parameters of Weibull distribution reflects the product failure characteristics, so the Weibull distribution is also quite widely used, while mission reliability affects the performance of the system's mission-related applications and is a key factor in determining whether the product can perform its mission successfully. (4) For different calculation models, mission reliability firstly establishes mission profiles based on mission descriptions, and for different missions, a system may have multiple mission profiles, based on which multiple mission reliability models are generated. In contrast, when calculating the basic reliability of a system, a system corresponds to only one reliability calculation model.

The theoretical bases of traditional research on network reliability assessment can be divided into three types: mathematical analysis methods based on graph theory and probability theory, simulation methods that simulate random events, and field experiment methods based on real scenarios. Figure 1 shows the theoretical bases and research methods of traditional network reliability assessment methods.

Connectivity reliability is the first proposed network reliability metric and is classified into active and passive networks based on the presence or absence of specified source points in the network. The classical analytical algorithms for computing network connectivity reliability include state enumeration, exclusion principle, disjoint sum, factorization, graph transformation, and delimitation methods. These algorithms usually assume that the links have only two states, fault and normal, and that the probabilities of link failures in the network are independent of each other. Network reliability design needs to consider redundancy design, fault management and prevention, data management, node and link trustworthiness, environment, destruction resistance, security, and other factors. The capacity of a link is limited at the time of transmission, and the capacity reliability refers to the probability of success in transmitting the required capacity between the two ends of the link after setting the maximum capacity for each link, as shown in the following equation:

$$P(\theta \mid k) = \frac{\int \alpha \cdot (\theta - \mu)/\sigma d\theta}{kr}. \tag{1}$$

This type of algorithm adds capacity constraints to the consideration of topological connectivity, and this network model has evolved into the "random flow network model":

$$\text{limit}C = \frac{1}{n}(3.36 + \varsigma)^3 + C_0. \tag{2}$$

Based on this model, researchers have proposed a series of computational methods. The capacity reliability assessment model is based on known conditions, such as node and link reliability information (e.g., reliability), node and link capacity information, network topology, and transmission capacity requirements, to solve for the probability of the existence of a connectivity path that satisfies certain capacity requirements for some set of nodes [20]. The connectivity reliability assessment classification is shown in Figure 2.

Performance reliability focuses on the traffic on the network path, and the physical links and capacity are mapped to the traffic path during the evaluation process, which can concisely reflect the performance degradation of the network. When evaluating the network performance reliability, the probability that the information from the source node reaches the destination node within the specified time is taken as the timely reliability of this network, the probability that the routing buffer overflows is used as a criterion to evaluate the network congestion, and the ratio of packet

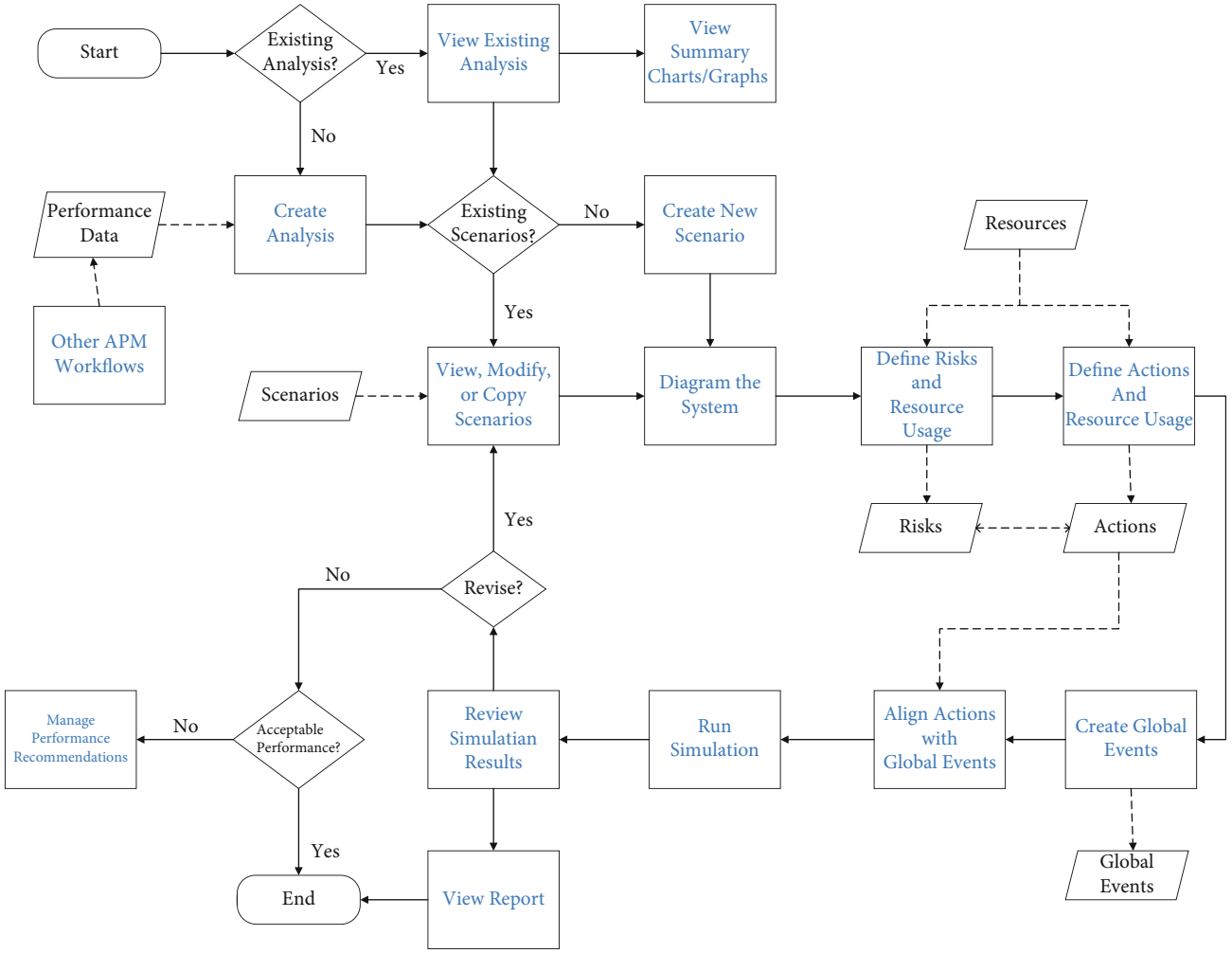

Figure 1: Classification of network reliability assessment methods.

reception at the receiving end to the amount sent at the sending end can also be used as the complete reliability of this network. Although the above three types of network reliability assessment of connectivity reliability, capacity reliability, and performance reliability can reflect the different functional requirements, metric range, and network performance of the network, it is difficult to give the comprehensive capability of the network when it is running a task. The problem of a comprehensive assessment of task-centric network reliability can be formulated as follows:

$$Y = \bigcap_{i=1}^{n} X_i + \bigcap_{i=1}^{r} U_i + c. \tag{3}$$

Many different types of lifetime distributions are used in reliability engineering, classified as discrete and continuous. Discrete distributions include mainly binomial, geometric, and Poisson distributions, and discrete distributions include mainly exponential, Weibull, normal, and log-normal distributions. The exponential distribution of continuous type is the most important type of distribution in reliability statistics and is almost exclusively used to describe the reliability of electronic equipment. The failure rate in the exponential distribution is constant and independent of time. Since the beginning of reliability studies, the exponential distribution has been the most widely used, and it has a large number of advantages such as simplicity of calculation, ease of estimation of parameters, and additivity of the failure rate, and when the failures of the components in a system satisfy the exponential distribution, its system also satisfies the exponential distribution. The continuous type of Weibull distribution and other distributions are all more closely related, and the range of values of the shape parameter of the Weibull distribution reflects the failure characteristics of the product, so the Weibull distribution is also used quite widely [21]. In this paper, the two typical continuous-type distributions that are most widely used for sensor life distribution are chosen as exponential distribution and Weibull distribution. The exponential distribution is shown in equation (4), and the Weibull distribution is shown in equation (5):

$$F(x) = \begin{cases} \lambda e^{-\lambda x}, & x > 0, \\ 0, & x \le 0, \end{cases} \tag{4}$$

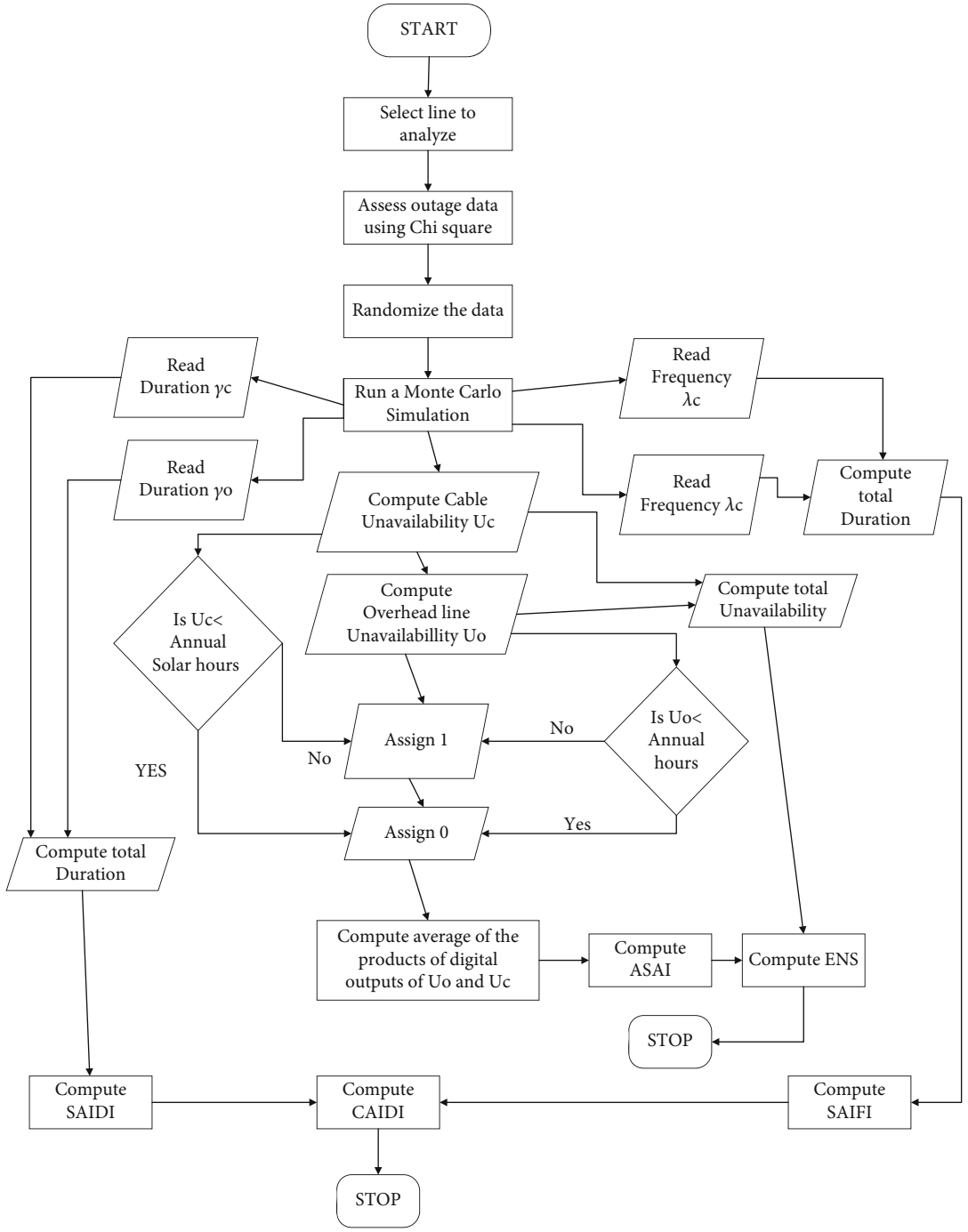

Figure 2: Classification of connectivity reliability assessment.

$$F(x) = \begin{cases} re^{-x} + \mu x, & x > 0, \\ 0, & x \le 0. \end{cases} \quad (5)$$

For WSN reliability studies, the star network topology is simple, with two-way communication between the sensor nodes and the Sink (or base station), but no communication path is established between the nodes. In addition, the data information from the sensor nodes can be sent directly to the base station, so the failure of the nodes can directly affect the normal operation of the WSN. All these advantages are good for assessing the reliability of WSNs, and the study of WSN reliability fruits of star network topology also has great reference value for later study of other network topologies. Therefore, in the WSN reliability study in this paper, the wireless sensor network topology is a star network.

The network reliability design needs to consider redundancy design, fault management and prevention, data management, node and link trustworthiness, environment,

resilience to destruction, security, and other factors. The following aspects should be considered in focus: (1) Redundancy design. Focus on considering the redundancy of key equipment and links. Decentralized deployment of multiple key devices in the same area to achieve load sharing and decentralized multiple means and multiple routing protocols are implemented on the transmission path. (2) Network protection mechanisms. For example, reliable routing protocols, hot backup protocols, route binding protocols, and automatic protection switching protocols are commonly used network protection mechanisms. (3) Fault-tolerant design. That is, the network is robustly designed so that it can still work properly or partially work in case of some errors or failures. The transmission path is selected by considering the remaining energy of neighboring nodes, data transmission distance, and network load balancing to reduce the chance of individual path overheating, reduce the probability of too many shared nodes, balance the network energy consumption, and improve the data transmission success rate and network lifetime. The main methods are fault limiting, fault detection, fault shielding, retry techniques, fault diagnosis, reorganization, recovery, reconfiguration, etc. (4) Congestion control. Through analysis or reliability simulation test to find out the "bottleneck" of network traffic, taking effective congestion control strategy can increase network resources and reduce user demand from two aspects to consider to solve the congestion problem. (5) Online maintenance guarantee design, that is, without interrupting the network operation, the maintenance, and protection of the network. Commonly used methods include hot-plug replacement of hardware and online upgrade of software. (6) Simulation-assisted design, through the network reliability simulation test method, the network completeness, resistance to destruction, availability, recovery, reliability of the auxiliary analysis, and design.

3.2. Data Transmission Reliability Analysis of Wireless Sensor Networks for Social Network Optimization. In the PPSSN model, there is a data owner (DO), a DO server, an attribute management server (AMS), an access user, and a social network platform (SNP). The DO server encrypts and stores the DO's buddy list, queries the encrypted list when the user requests access to the data, and returns the buddy relationship data, which shares the DO's overhead but does not affect the security of the data. After receiving a user's access request, the attribute management server (AMS) requests a buddy relationship from the DO, determines the buddy relationship from the data returned by the DO, and distributes the private key to the access requestor. The social network service platform SNP is the data distribution platform for users. Visitor V is a user of the social network platform and needs to obtain the appropriate access rights to access the data on the SNP when viewing the data published by the DO. When a visitor requests access to the data, he/she first needs to send a request to DO and can access the SNP data only after passing the authentication of AMS and DO and receiving the private key. Users who are not DO friends can only access the data that was last published on the SNP, and illegal users who are identified by AMS as social networks cannot access any DO publication data.

According to the extended complex network model of social networks, the concept of multiconstraint path pattern matching is proposed, i.e., finding matches in the data graph that match the pattern graph. Based on the multiconstraint optimized path selection algorithm, the multiconstraint edge matching algorithm is executed for each edge in the pattern graph, and the query results obtained are connected in the order in the pattern graph to form answers that match the user's query conditions. To improve the execution efficiency and connection efficiency, a probability-based sampling estimation algorithm is introduced to accelerate the execution of the path matching algorithm and also to provide guidance for the mapping query result connection algorithm [22]. The algorithm can be applied to pattern matching in areas such as location-based social networks, spatial crowdsourcing, and recommender systems.

Since the wireless communication link quality sequence characterized by the signal-to-noise ratio is characterized by the superposition of smooth and noisy sequences, the time series prediction model lacks accuracy for the prediction of sequence values. Therefore, in this paper, according to the complex environment of the energy grid, and combined with the characteristics of wireless communication link quality S/N sequence, a prediction algorithm based on LSTM for the confidence interval of communication link reliability is proposed, and the structure diagram is shown in Figure 3.

In this paper, we measure the attribute similarity between two users by determining whether the attribute content is the same. When matching whether the attribute contents are the same, the birthday attribute is matched only to the year, and the address and hometown are matched only to the city, and then, the result of whether these nine attributes match is defined as a nine-dimensional vector. In this vector, if the attribute contents are the same, the corresponding element has a value of 1; otherwise, the value is 0. The reason for considering names and avatars is that if the avatars and names of two accounts are very similar or identical, there is a high probability that they represent a particularly close relationship, usually a couple or the same user with multiple accounts. In determining whether avatars are similar, this paper chooses to use the perceptual hashing algorithm because avatar files are usually small. In existing studies on attribute inference, user identity linking, and link inference, the most basic approach is based on the principle of homogeneity, i.e., the information between users and their surrounding friends is similar, and the closer the friends, the higher the degree of similarity, so that the target user's undisclosed information can be inferred from the information disclosed by surrounding friends. Connectivity reliability is the first proposed network reliability index, which is divided into active and passive networks according to the presence or absence of specified source points in the network. The classical analytical algorithms for computing network connectivity reliability include state enumeration, exclusion principle, disjoint product sum, factorization, graph transformation, and delimitation method. These

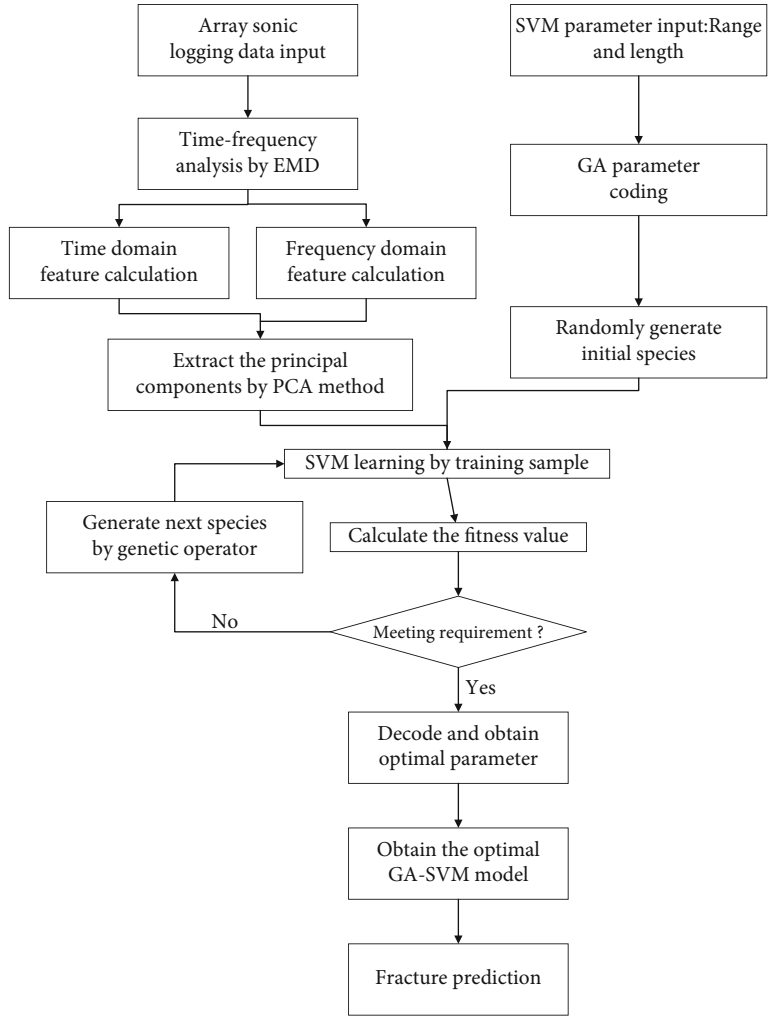

Figure 3: Confidence interval prediction algorithm for communication link reliability.

algorithms usually assume that the links have only two states, fault and normal, and the probabilities of link failures in the network are independent of each other. The most direct and effective way of this is to compare the attribute information filled in the profile of the user. Based on the above principles, this paper argues that the same attribute information between the target user and his friends is very likely to reveal the user's private information, and even if the target user himself does not disclose this information, a malicious attacker can still infer the target user's information based on the attribute content of the largest number of the same friends around. The closeness between any two participants also has similar properties as trustworthiness: self-reflexivity, asymmetry, dynamism, complexity, and transferability (not to be elaborated here). There is no subjectivity and it possesses objectivity, as the closeness is based on the interaction behaviour of the participants and can be analyzed by data mining techniques. In addition to this, it is also decaying, showing a tendency to decay as the path length increases.

When considering the spatial relationships and social identities of the participants, the following search process needs to be executed: the first step: all the nodes in the network need to be traversed to find the nodes that satisfy the location information and text information; the second step: among these nodes, find the paths in the network that meet the multiple constraints according to the multiple constraints specified by the user using one of the nodes as the source node and the other node as the target node. But with the increase in the number of nodes, the first step becomes very difficult, so the algorithm proposed above is no longer good enough to solve the optimal path selection problem for multiple constraints based on geographic location, and the search space is reduced based on location information and text information for solving the optimal path selection problem for multiple constraints regarding spatial constraints and social constraints. To speed up the filtering of geolocation information and text information, spatial text indexes need to be created for participants in social networks. Spatial text indexing can be classified as spatial indexing, text indexing, and hybrid indexing. Depending on the priority of spatial and text indexes, they can be classified as text-first and spatial-first. Text-first usually uses the inverted file as the top-level index and then arranges

each posting list in the inverted list by a spatial structure, which can be an R-Tree, a grid, or a space-filling curve. And spatial-first usually uses the spatial structure as the top-level index, with leaf nodes (or grid cells) containing inverted files or bitmaps of the object's textual information. There is also a tight combination of both indexes so that both types of information can be trimmed from the search space during the search.

4. Experimental Verification and Conclusion

The dataset used in this paper contains 2626 objects, each record contains the participant's sequence number, nickname, key text information extracted from the tweet, and the participant's spatial geographic location information (latitude and longitude). The constraint values of trust, closeness, and reputation of the participants are randomly generated through the WS small-world model. The specific generation process is as follows: (1) the network contains N (N randomly taken as 150, 300, 450, 600, 750, and 1050) nodes, and each node connects m edges (m randomly taken as 1~8) with its nearest m nodes; (2) an edge is added between a randomly selected pair of nodes with probability pr (pr randomly taken as 0.1~0.8), and any two different nodes have at most one edge between them, and each node cannot be connected to itself. The above procedure was repeatedly performed, and 24 subdatasets were synthesized. In the simulation experiments, the trust, closeness, and reputation values between participants were randomly generated, and to better model the decay of closeness in social networks, the decay factor was set to $\delta = 1.5$, and the source participants specified the bound values of trust, closeness, and reputation as $\{0.05, 0.001, 0.3\}$. The privacy data in social networks mainly includes users' identity information, login information, friend information, and the content published on social network platforms and information dissemination. The purpose of setting the parameters in this way is to allow more paths to satisfy the constraints. The weights of trust, intimacy, and reputation in the path quality function are $\{0.25, 0.25, 0.5\}$, highlighting the importance of reputation in trust assessment.

The IR-Tree-MBS algorithm is compared with the H_MCOP algorithm and the MBS algorithm, respectively. The three algorithms perform the same path query condition three times on each of the 24 randomly generated subdatasets, and each query needs to be repeated three times for averaging. Comparing the path quality and path query efficiency found by the algorithms, Figure 4 shows the comparison results of path quality.

The R-Tree-MBS algorithm and the MBS algorithm have similar path lookup quality because both algorithms use the same lookup strategy and objective function. The path quality of both algorithms is no worse than that of the H_MCOP algorithm, which is because the IR-Tree-MBS algorithm, MBS algorithm, and H_MCOP algorithm all treat the path found as optimal when it has the maximum path quality and is a feasible solution, which leads to similar pathfinding quality when finding certain paths (e.g., on datasets 9 and 15 in Figure 4). When there is a maximum path quality and it is

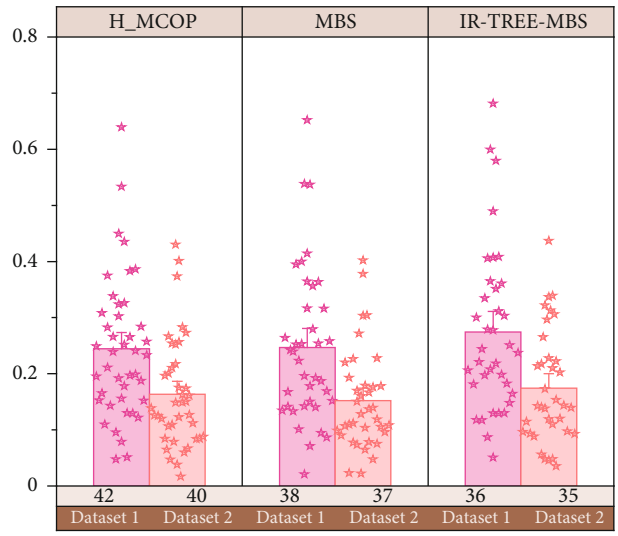

Figure 4: Comparison of path quality finding results of different algorithms on different datasets.

not a feasible solution, the H_MCOP algorithm stops searching according to the minimum cost and starts searching according to the minimum objective function $g\lambda(p) < 1$. This leads to the phenomenon that the H_MCOP algorithm cannot find the near-optimal solution or even actually has a feasible solution but H_MCOP returns no feasible solution, while the MBS and IR-Tree-MBS algorithms can find approximately optimal solutions.

From Figure 5, we can see that the H_MCOP algorithm and the MBS algorithm have higher execution efficiency when the network size is not large and the network structure is relatively simple, while the IR-Tree-MBS algorithm is relatively poor. This is because the IR-Tree-MBS algorithm needs to create IR-Tree indexes of the nodes in the network first when it is executed, which consumes about 1-5 seconds. The discrete distribution mainly includes binomial distribution, geometric distribution, and Poisson distribution. The discrete distribution mainly includes exponential distribution, Weibull distribution, normal distribution, and log-normal distribution. When the network size is small, the algorithms MBS and H_MCOP algorithms for the direct query have higher efficiency. However, as the network size increases and the complexity of the network structure increases, the efficiency of the H_MCOP algorithm and MBS algorithm gradually decreases, while the IR-Tree-MBS algorithm has good stability. The reasons include two aspects: (1) the IR-Tree-MBS algorithm utilizes the characteristics of the IR-Tree structure and does not query the path directly but performs distance pruning and keyword pruning first, narrowing the search scope to a certain extent, which is not considered by the H_MCOP algorithm and the MBS algorithm; (2) the IR-Tree-MBS algorithm does not need to be like the H_MCOP algorithm to compute $g\lambda(p) > 1$ during the forward search, especially when λ tends to ∞, resulting in a larger time overhead.

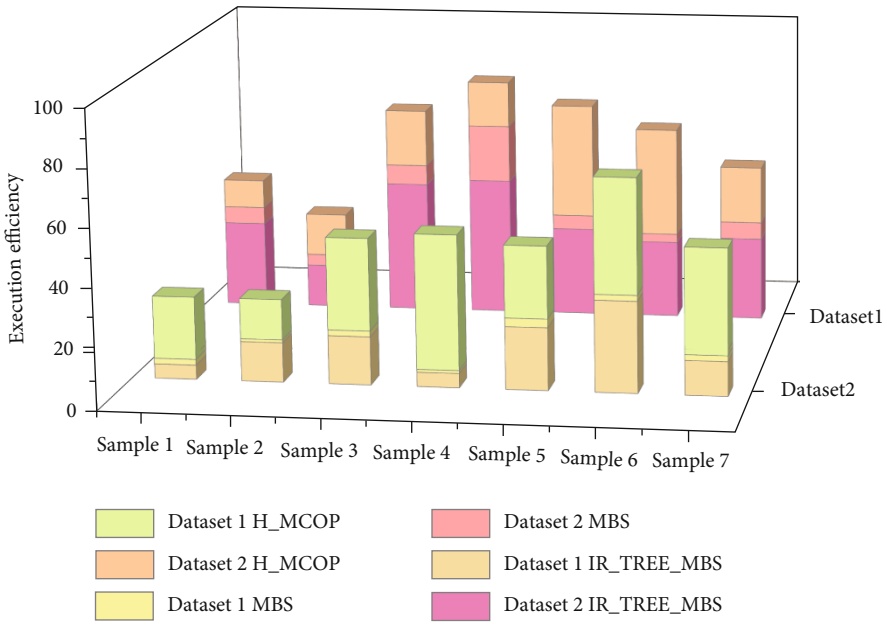

Figure 5: Execution efficiency of different algorithms on different datasets.

From Figure 6, we know that as the number of network polling increases, the total energy consumption of the network increases regardless of whether it is 100 nodes or 200 nodes, and the increase in energy consumption is greater for the AODV-SMS route recovery protocol, followed by AODV-SMS (PSO), and AODV-SMS (ABC-PSO) has the least energy consumption. And it is also seen that as the number of sensing nodes in the network increases, along with it, the density of the whole network increases, the AODV-SMS route recovery method has a single transmission path and the sensing nodes that die faster during the source node transmission are generally in the common node, the transmission path where the common node is located, and the location near the destination node Sink. At the same time, as the density of sensing nodes increases, the probability of using the same transmission path increases greatly, and the energy consumption of the common node on the same transmission path is very large, which is prone to premature "death" phenomenon, resulting in data loss and data transmission link interruption. The AODV-SMS (ABC-PSO) multipath routing recovery mechanism proposed in this paper considers the remaining energy of neighboring nodes, data transmission distance, and network load balancing in the process of the data transmission path which reduces the chance of individual path overheating, decreases the probability of too many shared nodes, balances the network nodes, balances network energy consumption, and improves data transmission success rate and network lifetime.

As can be seen from Figure 7, the energy utilization of the algorithm proposed in this paper is much higher than that of the AODV-SMS routing protocol, mainly because the adopted AODV-SMS (ABC-PSO) route recovery strategy interrupts the original data transmission path as the Sink moves; it searches for the nearest transmission path near the original path and considers the network energy consumption equalization, which makes the energy consumption of our proposed route recovery strategy lower than that of other methods. When considering the spatial relationships and social identities of participants, the following search process needs to be performed: Step 1: all nodes in the network need to be traversed to find nodes that satisfy the location information and text information; Step 2: among these nodes, one of them is used as the source node and the other as the target node to find paths in the network that meet the multiple constraints according to the multiple constraints specified by the user. Although the swarm intelligent optimization algorithm AODV-SMS (ABC-PSO) consumes a portion of energy to optimize the data transmission path, considering the remaining energy of neighboring nodes, data transmission distance, and network load balancing, the proposed multipath transmission route recovery strategy can make full use of the information provided by the original path to quickly recover an efficient and reliable transmission path, providing faster global convergence for network optimization.

As can be seen from Figure 8, the end-to-end transmission delay of the AODV-SMS protocol at a low number of nodes (100 nodes) is higher than the original. AODV-SMS (PSO) and AODV-SMS (ABC-PSO) multipath routing recovery path mechanisms are slightly larger. Mainly because the data transmission congestion is not serious in the case of the low number of nodes, the difference in transmission delay between AODV-SMS (PSO) and AODV-SMS (ABC-PSO) multipath transmission route recovery mechanisms is not significant, and the end-to-end delay of the proposed algorithm is smaller than that of the AODV-SMS method. It is also observed that as the number of sensing nodes increases, the multipath route recovery mechanism of AODV-SMS (PSO) and AODV-SMS (ABC-PSO)

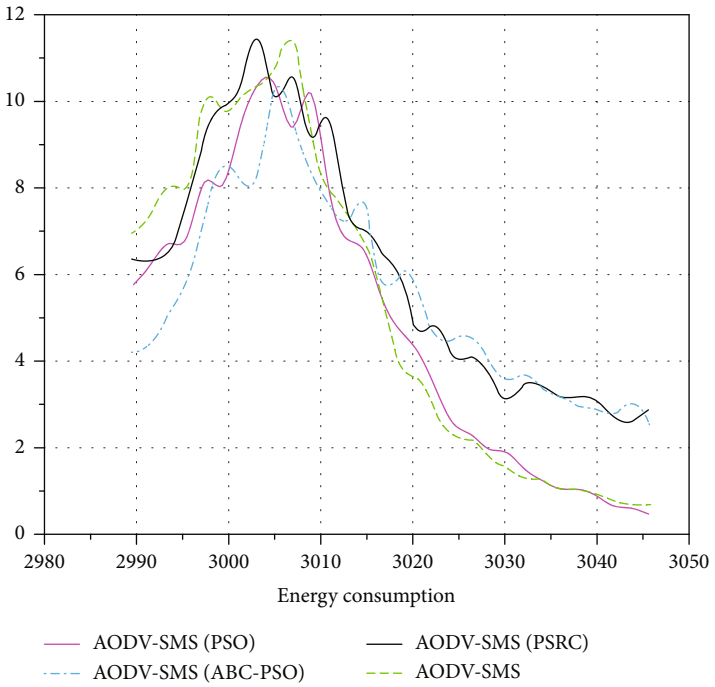

Figure 6: Network energy consumption comparison.

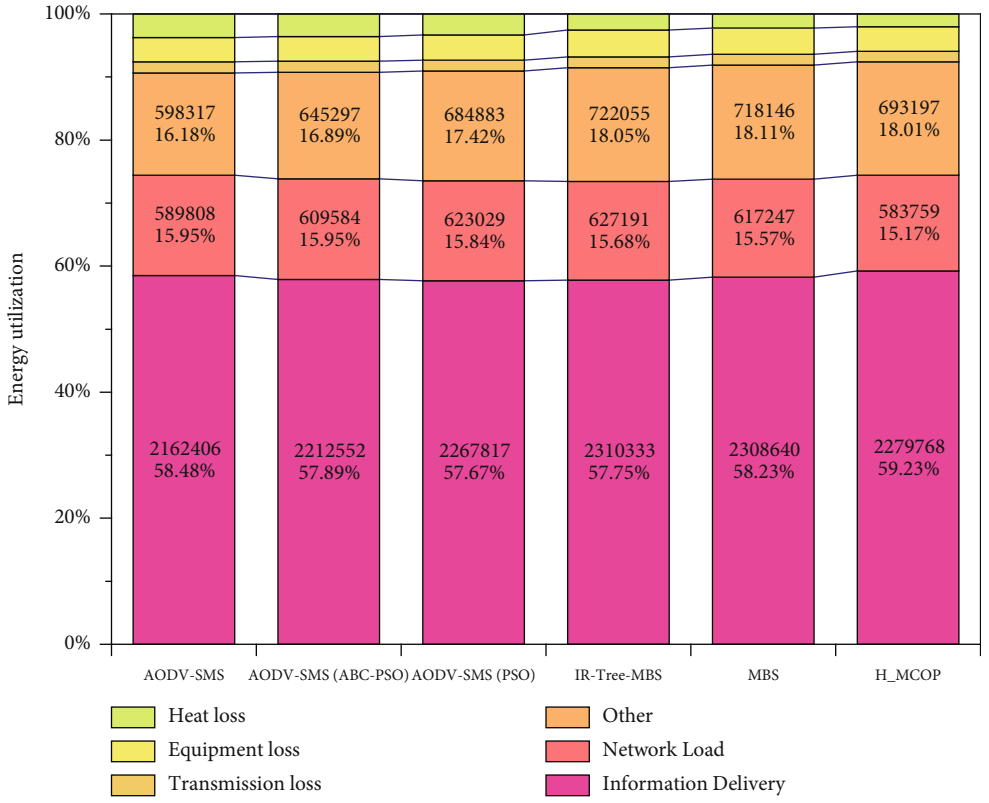

Figure 7: Algorithm energy utilization.

algorithms increases the number of transmission paths to the destination node, while the new transmission paths are constructed with comprehensive consideration of transmission AODV-SMS (ABC-PSO) routing recovery protocol showing a better packet transmission delay time than other routing recovery strategies. Packet transmission delay takes less time, and there is an increasing difference between them. This is enough to show that the larger the network size, the

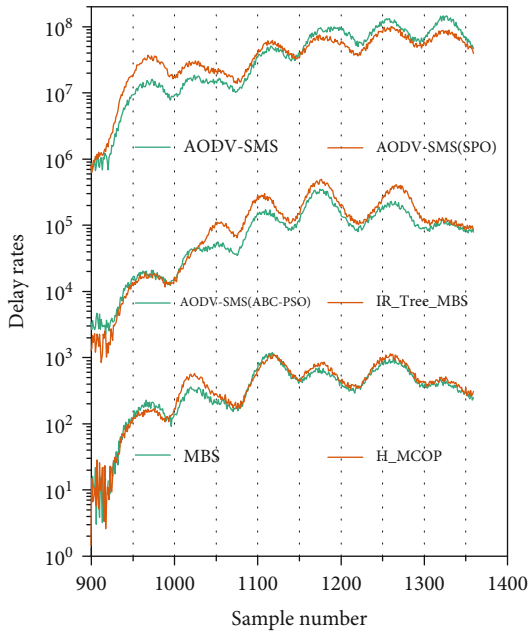

Figure 8: Comparison of network propagation delay rates.

greater the delay and transmission path length spent by the source node to transmit to the destination node, which better reflects the advantage that the multipath route recovery strategy proposed in this paper can consider the remaining energy of the neighboring nodes of the transmission link and the communication distance and the network load balance, select more suitable communication nodes to form a better alternative path, and make the network energy consumption have more balanced distribution and the longest lifetime.

5. Conclusion

With the convenience of people communicating with each other in the information age, social networks have been created and gradually become popular. Due to their convenience and easy operation, social networks have become deeply involved in people's lives and work in the context of increasingly mature network technology. At the same time, the issue of privacy in social networks has also gradually aroused people's concern. The root cause of the private security problem in social networks is that the private data of the data owner is spread on the social network platform without the direct physical control of the data owner, so it may cause the leakage of the data, which makes the users who originally do not have the access permission or even the users who maliciously steal the information to view the content published by the data owner.

In this paper, by studying the network reliability problem differently from the general study of reliability content (network failure rate, fault diagnosis, fault repair, etc.), we conduct a comprehensive study of network performance (network energy consumption, load balancing, transmission delay, network connectivity, reliability, etc.). By introducing intelligent optimization methods and artificial intelligence algorithms, we address reliability issues such as basic research on mobile wireless sensor network fault prediction and network reliability assessment methods, the impact of mobile path optimization on data collection efficiency and network reliability, reliable data transmission based on data fusion methods, and intelligent fault tolerance algorithms for multipath routing to reduce fault interference and network energy consumption, improve network efficiency, and increase network connectivity, availability, and reliability and extend the network survival cycle as the objectives to ensure energy-efficient, efficient, and reliable operation of mobile wireless sensor networks in complex application environments. The discrete distribution mainly includes binomial distribution, geometric distribution, and Poisson distribution. The discrete distribution mainly includes exponential distribution, Weibull distribution, normal distribution, and log-normal distribution. In the key issuance process of attribute encryption, the management of user rights is jointly implemented by the data owner and the attribute management server, which not only reduces the overhead of the data owner but also avoids collusion attacks between the attribute management server and illegally accessed users. To weigh the usability of data distribution and the security of information privacy protection, users are classified and designed to achieve access control for different users with different privileges. In addition to this, the caching mechanism of the buddy data is designed to improve and optimize the original scheme and reduce the decryption overhead. The model improves query efficiency, reduces the system overhead, and enhances privacy security.

Data Availability

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

Conflicts of Interest

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

References

[1] J. Lu, L. Feng, J. Yang, M. M. Hassan, A. Alelaiwi, and I. Humar, "Artificial agent: the fusion of artificial intelligence and a mobile agent for energy-efficient traffic control in wireless sensor networks," *Future Generation Computer Systems*, vol. 95, pp. 45–51, 2019.

[2] F. Zhang, "Research on reliability analysis of computer network based on intelligent cloud computing method," *International Journal of Computers and Applications*, vol. 41, no. 4, pp. 283–288, 2019.

[3] A. Alarifi and A. Tolba, "Optimizing the network energy of cloud assisted internet of things by using the adaptive neural learning approach in wireless sensor networks," *Computers in Industry*, vol. 106, pp. 133–141, 2019.

[4] R. P. M. Sundhari and K. Jaikumar, "IoT assisted hierarchical computation strategic making (HCSM) and dynamic stochastic optimization technique (DSOT) for energy optimization in

wireless sensor networks for smart city monitoring," *Computer Communications*, vol. 150, pp. 226–234, 2020.

[5] 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.

[6] J. Tan, W. Liu, T. Wang et al., "An adaptive collection scheme-based matrix completion for data gathering in energy-harvesting wireless sensor networks," *IEEE Access*, vol. 7, pp. 6703–6723, 2019.

[7] S. Randhawa and S. Jain, "MLBC: multi-objective load balancing clustering technique in wireless sensor networks," *Applied Soft Computing*, vol. 74, pp. 66–89, 2019.

[8] M. Faheem, R. A. Butt, B. Raza et al., "FFRP: dynamic firefly mating optimization inspired energy efficient routing protocol for internet of underwater wireless sensor networks," *IEEE Access*, vol. 8, pp. 39587–39604, 2020.

[9] B. Pitchaimanickam and G. Murugaboopathi, "A hybrid firefly algorithm with particle swarm optimization for energy efficient optimal cluster head selection in wireless sensor networks," *Neural Computing and Applications*, vol. 32, no. 12, pp. 7709–7723, 2020.

[10] S. E. Mood and M. M. Javidi, "Rank-based gravitational search algorithm: a novel nature-inspired optimization algorithm for wireless sensor networks clustering," *Cognitive Computation*, vol. 11, no. 5, pp. 719–734, 2019.

[11] 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.

[12] R. Elhabyan, W. Shi, and M. St-Hilaire, "Coverage protocols for wireless sensor networks: review and future directions," *Journal of Communications and Networks*, vol. 21, no. 1, pp. 45–60, 2019.

[13] 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.

[14] M. E. Ekpenyong, D. E. Asuquo, and I. J. Umoren, "Evolutionary optimisation of energy-efficient communication in wireless sensor networks," *International Journal of Wireless Information Networks*, vol. 26, no. 4, pp. 344–366, 2019.

[15] 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.

[16] O. Deepa and J. Suguna, "An optimized QoS-based clustering with multipath routing protocol for wireless sensor networks," *Journal of King Saud University-Computer and Information Sciences*, vol. 32, no. 7, pp. 763–774, 2020.

[17] S. Sivakumar and P. Vivekanandan, "Efficient fault-tolerant routing in IoT wireless sensor networks based on path graph flow modeling with Marchenko–Pastur distribution (EFT-PMD)," *Wireless Networks*, vol. 26, no. 6, pp. 4543–4555, 2020.

[18] X. Liu, T. Qiu, and T. Wang, "Load-balanced data dissemination for wireless sensor networks: a nature-inspired approach," *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9256–9265, 2019.

[19] G.-D. Zhou, M.-X. Xie, T.-H. Yi, and H.-N. Li, "Optimal wireless sensor network configuration for structural monitoring using automatic-learning firefly algorithm," *Advances in Structural Engineering*, vol. 22, no. 4, pp. 907–918, 2019.

[20] J. Jiang, X. Zhu, G. Han, M. Guizani, and L. Shu, "A dynamic trust evaluation and update mechanism based on C4. 5 decision tree in underwater wireless sensor networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 9031–9040, 2020.

[21] A. Seyfollahi and A. Ghaffari, "Reliable data dissemination for the Internet of Things using Harris hawks optimization," *Peer-to-Peer Networking and Applications*, vol. 13, no. 6, pp. 1886–1902, 2020.

[22] S. Tabatabaei, A. Rajaei, and A. M. Rigi, "A novel energy-aware clustering method via lion pride optimizer algorithm (LPO) and fuzzy logic in wireless sensor networks (WSNs)," *Wireless Personal Communications*, vol. 108, no. 3, pp. 1803–1825, 2019.