Data Security Sharing Method of Opportunistic Network Routing Nodes Based on Knowledge Graph and Big Data

Xucheng Wan and Yan Zhao(✉)

Ningbo City College of Vocational Technology, Ningbo 315199, China
zhaoyan48513@163.com

Abstract. Opportunity network is one of the main network types for data sharing applications today. Due to the completely self-organized and distributed characteristics of its own structure, there is a greater security risk in the process of data sharing. Therefore, an opportunity based on knowledge graph and big data is proposed. Research on data security sharing method of network routing nodes. Analyze the opportunistic network routing protocol, expound the data sharing mode of the opportunistic network routing nodes, represent the opportunistic network based on the knowledge graph, calculate the influence degree parameter of the routing node, build the routing node influence propagation model based on this, formulate the routing node data publishing/subscribing rules, combined with Secure multi-party computing big data builds a routing node data security sharing architecture to realize the secure sharing of opportunistic network routing node data. The experimental results show that after the method is applied, the minimum value of the shared data packet loss rate reaches 4%, and the maximum value of the data sharing safety factor reaches 0.98, which fully confirms that the method has a better data security sharing effect.

Keywords: Knowledge Graph · Big Data · Opportunistic Network · Routing Node · Data Security · Data Sharing

1 Introduction

Opportunistic network integrates multiple concepts such as delay-tolerant network, self-organizing network and social network. It uses the encounter opportunities in people's daily life to transmit and share messages, so as to achieve efficient networking and message delivery in harsh network environments. With the increasing popularity of a large number of inexpensive short-range handheld communication devices (such as mobile phones, iPads, Tablets, etc.) in recent years, opportunistic networks have also received more and more attention. Opportunistic network is a kind of self-organizing delay-tolerant and interruption-tolerant network in which the link is in the intermittent connection state for a long time, and uses the encounter opportunity brought by its own movement to realize message transmission. Opportunity network has the characteristics

B. Wang et al. (Eds.): ICMTEL 2023, LNICST 534, pp. 139–154, 2024.
https://doi.org/10.1007/978-3-031-50577-5_11

of people-centered social network. It explores and develops the social relationship and movement laws between people, and carries out efficient message sharing and transmission. It eliminates the communication barriers caused by node mobility in traditional networks. Opportunistic networks treat each movement of a node as a new transmission opportunity. It is precisely because opportunistic networks have different design concepts and processing methods than traditional wireless networks in the face of disconnection, delay, and node movement, which makes opportunistic networks have wider application requirements [1].

In addition, opportunistic networks have some properties of MANET due to their completely self-organizing and distributed architecture. In the MANET architecture, data transmission between mobile nodes relies on the end-to-end routing path established by the AODV or DSR routing algorithm. However, in the actual self-organizing network environment, due to the frequent high-speed movement of nodes, extremely sparse density, signal battery attenuation and other problems, a large number of nodes in the network are in a disconnected state, resulting in a long-term intermittent network connection. A complete and effective end-to-end communication path cannot be established between nodes. Unlike MANET, opportunistic networks do not assume a complete end-to-end path between nodes. Nodes only use local information to calculate and select an appropriate next-hop route, expecting to pass messages through the movement and data forwarding of multiple nodes. to the destination node. Furthermore, opportunistic networks do not need to acquire topology information for the entire network. Therefore, opportunistic networks have better availability and adaptability in the face of harsh environments. Especially nowadays, the popularity of a large number of low-cost handheld devices with various communication modules makes it possible for people to realize the transmission and sharing of information by forming a network by themselves through various encounter opportunities.

In an opportunistic network, nodes implement message transmission in a "store-carry-forward" manner, and there is no need for a complete communication link between the source node and the destination node. Mobile nodes use local knowledge for routing selection without acquiring any network topology information. The routing problem in traditional wireless mobile networks has evolved into a simple forwarding node selection strategy problem in opportunistic networks. However, routing is still one of the core hardware in opportunistic networks. For an opportunistic network, the transmission of data depends on the encounter opportunities brought by the movement of nodes to reach the destination node in a multi-hop manner. Therefore, how to choose the most ideal forwarding target and the most ideal forwarding timing has become the core issue of the data transmission mechanism in opportunistic networks, and is also the key to the security of data sharing.

Due to the uncertainty of the forwarding target of opportunistic networks, the shared security of routing nodes is affected by many factors, such as the security of route selection and the security of node movement. With the expansion of the application scope of opportunistic networks, the data sharing security problem has gradually emerged, which has attracted widespread attention from the public and has become one of the main obstacles to restrict the development and application of opportunistic networks. Therefore, an opportunistic network based on knowledge graph and big data is proposed.

Research on data security sharing method of routing nodes. It is hoped that through the application of knowledge graph and big data technology, the security of data sharing of routing nodes in opportunistic networks will be improved, and sufficient power support will be provided for the sustainable development of opportunistic networks.

2 Research on Data Security Sharing Method of Routing Nodes

2.1 Analysis of Opportunistic Network Routing Protocols

In order to improve the security of data sharing of opportunistic network routing nodes, the first step is to analyze the opportunistic network routing protocol, and lay a solid foundation for the construction of the subsequent routing node influence propagation model.

The opportunistic network routing pattern is shown in Fig. 1.

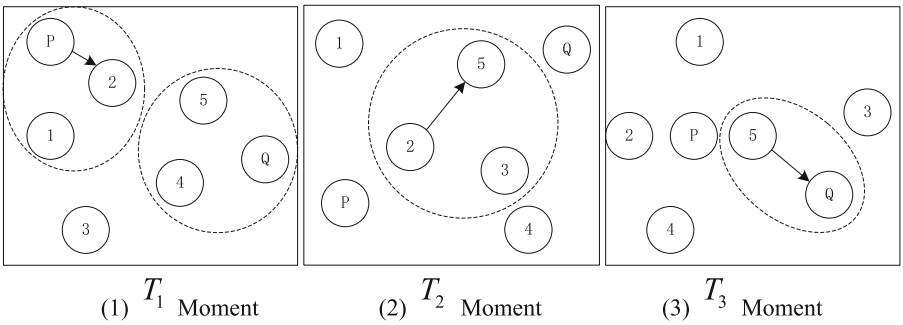

Fig. 1. Schematic diagram of opportunistic network routing mode

As shown in Fig. 1, node P sends a message to node Q at time T_1, but it cannot realize end-to-end transmission because it is not in the same connected domain. Therefore, the node P first compares the encounter probability between the neighbor nodes within the communication range and the destination node Q, and then forwards the message to the node 2 with a larger encounter probability. At time T_2, node 2 meets node 5, and finds that node 5 has a higher probability of encountering the destination node Q than itself, so node 2 forwards the message to node 5. Until time T_3, node 5 just meets node Q, so the message is finally delivered to the destination node.

According to different forwarding strategies, opportunistic network routing can be divided into four categories: scatter-based routing, utility-based routing, scatter-utility-based hybrid routing, and active mobility-based routing. Among them, the routing based on dissemination adopts the method of copying or encoding, and multiple copies of the message are transmitted in parallel through multiple paths in the network, thereby improving the efficiency of message transmission; the routing based on utility value adopts the method of single copy and single path. Use the information of nodes in the network or network state to evaluate, and select an appropriate forwarding node. The

corresponding routing evaluation function uses encounter prediction, context information, link status, etc. as parameters to calculate the probability that the target node will finally forward the message successfully; the routing based on the mixed utility value of the spread effectively integrates the characteristics of the above two routings. In the routing based on active mobility, the high-performance nodes deployed in a specific area of the network provide routing services for other nodes through active mobility, so as to realize the interactive communication of nodes in the network, compared with passively waiting for communication opportunities in ordinary wireless networks. Routing mode has better transmission performance [2].

The above process completes the analysis of the opportunistic network routing protocol, expounds the data sharing mode of the opportunistic network routing nodes, and provides support for the construction of the subsequent routing node influence propagation model.

2.2 Routing Node Affects the Propagation Model Construction

Based on the analysis results of the above opportunistic network routing protocol, the opportunistic network is represented based on the knowledge graph, and the influence degree of the routing nodes is analyzed.

Representing the opportunistic network in the form of a knowledge graph can effectively simplify the research process. The main performance parameters of the influence degree of routing nodes are degree, betweenness and Ψ_i value. Among them, the degree can represent the local importance of routing nodes. Defined as the sum of the number of all routing nodes connected to the current routing node, the expression is

$$\alpha_i = \sum\nolimits_i L_{(i)} \tag{1}$$

In formula (1), α_i represents the degree of routing node i; $L_{(i)}$ represents the routing node connected to the current routing node i; $\sum_i$ represents the sum of all routing nodes connected to the current routing node., and the summed result is expressed as the degree of the final routing node. It can be seen that the degree can represent the influence of the routing node in the local scope. However, we can also analyze that the disadvantage of degree indicating the influence of routing nodes is that the degree only considers the simplest structural information of the number of connections, and does not analyze the structural characteristics of the opportunistic network in depth. Therefore, there are some deficiencies in expressing the importance of routing nodes [3].

A more widely used measure of routing node importance than degree is betweenness. Betweenness considers structural properties to a certain extent more deeply than degree. To a certain extent, it can reflect the distance relationship between a routing node and other routing nodes in the network. When the betweenness value of the routing node is large, the average distance from the routing node to other routing nodes will be small. When the betweenness value of the routing node is small, the average distance between the routing node and other routing nodes will be large. The betweenness value is the manifestation of the propagation distance of the opportunistic network in the analysis of the importance of routing nodes, and the expression is:

$$\beta_i = \sum \frac{\chi_{jk}(i)}{\chi_{jk}} \tag{2}$$

In formula (2), β_i represents the betweenness of routing node i; χ_{jk} represents the number of shortest paths between any two routing nodes j and k in the opportunistic network; $\chi_{jk}(i)$ represents the number of χ_{jk} passing through node i. . By taking its ratio, the resulting value is the definition of the final betweenness.

In opportunistic network analysis, the most famous is the PageRank algorithm, which ranks the web page nodes by improving the degree index of the routing node and through the link form of the opportunistic web page nodes. Finally, the importance ranking of each routing node is obtained. In general, the PageRank algorithm is more inclined to be more important routing nodes, and the routing nodes it links to a relatively more important performance. The PageRank algorithm is shown in Fig. 2.

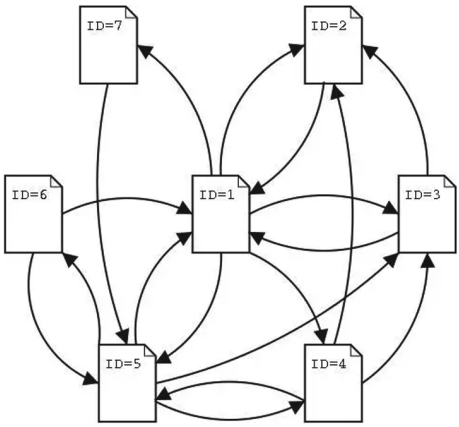

Fig. 2. PageRank algorithm

In the PageRank algorithm, the direction of each routing node link is actually the assignment of weights and the voting of importance. The PageRank value for a routing node is expressed as

$$\Psi_i = \delta * \frac{1}{n} + (1 - \delta) * \sum \frac{\beta_i}{\alpha_i} \tag{3}$$

In formula (3), Ψ_i represents the PageRank value of the routing node i; δ represents the damping factor, because in the link pointing, it is not always possible to visit the routing node with a 100% probability. Therefore, a certain probability is required to indicate the jumping situation of nodes; n represents the total number of routing nodes in the network. It can be seen from Eq. (3) that the link pointing behavior and voting behavior of the PageRank algorithm mainly occur in directed graphs. When dealing with undirected graphs, the edges between routing nodes provide less information, which is also PageRank. A shortcoming of the algorithm.

Since the above-mentioned parameters of the influence degree of routing nodes have their own shortcomings, they need to be integrated and applied. Based on this, a routing node influence propagation model is constructed, as shown in Fig. 3.

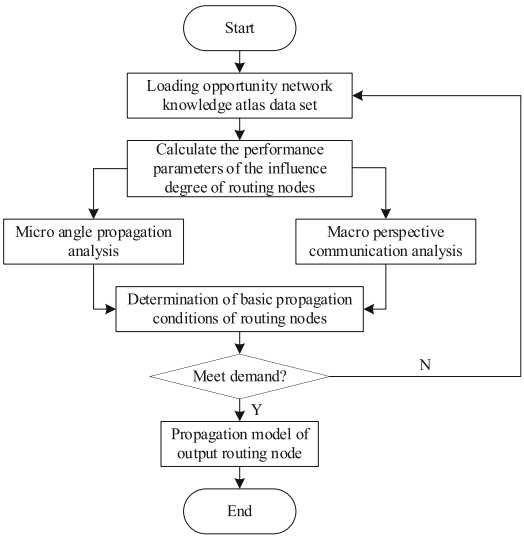

Fig. 3. Schematic diagram of routing node influence propagation model

As can be seen from Fig. 3, the routing node influence propagation model based on knowledge graph needs to first describe the influence of routing nodes, that is, which routing nodes have more important influence in the overall opportunistic network [4]. After analyzing the important routing nodes, we divide the community of the overall opportunistic network, and then improve the modeling and analysis of the propagation model from the macro and micro perspectives. Finally, the propagation effect of the global opportunistic network is described, including the basic information of the propagation process such as the time of propagation, the scope of propagation, and the state of final propagation.

The above process completes the construction of the routing node influence propagation model, which provides a certain support for the formulation of subsequent routing node data publishing/subscription rules.

2.3 Routing Node Data Publishing/subscription Rules Formulation

Based on the above-mentioned construction of the routing node impact propagation model, the routing node data publishing/subscription rules are formulated to make sufficient preparations for the final data security sharing architecture construction and implementation.

Since the opportunistic network implements message transmission in the mode of "store-carry-forward", mining influential routing nodes in the network is of great significance for improving the efficiency of message transmission and reducing communication consumption. Based on the measurement idea of entropy centrality, this research first proposes a local centrality measurement method, and then proposes a global entropy centrality measurement method for the selection of publish/subscribe routing nodes from a global perspective [5].

Given an opportunistic network $G(V_n, E_n)$, where V_n represents the set of routing nodes in the opportunistic network, and E_n represents the set of connection attributes between routing nodes in the opportunistic network. If the data distribution routing node at the most core position in the mining opportunity network, $e_{i,j} \in E_n$ represents whether there is a connection between routing nodes. Because people's movement behavior has certain social attributes, the number of encounters between people and acquaintances is significantly higher than the number of encounters with strangers, and the probability of people and acquaintances meeting again in the future is also higher than the probability of encountering strangers again. The most stable data distribution routing node in the mining opportunity network, $e_{i,j} \in E_n$ represents the number of encounters between routing nodes. This section first studies the local centrality of routing nodes. If the measured routing node has the best local center position, the routing node needs to have the most neighbor nodes; if the measured routing node has the most stable local centrality, the following three factors need to be considered: the most neighbor nodes, the largest number of encounters, The most evenly distributed number of encounters with neighbor nodes. In order to meet the above requirements, the theory of information entropy is used to define the connection distribution characteristics of routing node i and other routing nodes, and the connection distribution entropy of node i is expressed as

$$Z(i) = -\sum P\left(e_{i,j}\right) \log_2 P\left(e_{i,j}\right) \tag{4}$$

In formula (4), $Z(i)$ represents the connection distribution entropy of routing node i; $P\left(e_{i,j}\right)$ represents the encounter probability between node i and j.

From the calculation result of formula (4), it can be seen that when the routing node has the best local center position, the larger the entropy value is, the more the number of neighboring routing nodes is; when the routing node has the most stable local centrality, if the two routing nodes have the same number of neighbors, and the routing node with a larger entropy value indicates that the number of encounters is more evenly distributed. If two routing nodes have the same probability of encountering, the routing node with a larger entropy value indicates that the number of neighbors is greater [6]. Considering that the number of encounters is also one of the important indicators to measure the local centrality of routing nodes, according to the above analysis results, this section proposes the definition of local centrality of routing nodes based on the connection distribution entropy, which is expressed as

$$K(i) = \sum e_{i,j} * Z(i) \tag{5}$$

In formula (5), $K(i)$ represents the local centrality of routing nodes.

Then the calculation formula of the global entropy centrality of routing nodes is:

$$\gamma(i) = K(i) + \sum\nolimits_{j \in \tau^1(i)} K(i) + \sum\nolimits_{j \in \tau^2(i)} K(i) + \cdots + \sum\nolimits_{j \in \tau^M(i)} K(i) \tag{6}$$

In formula (6), $\gamma(i)$ represents the global entropy centrality of routing nodes; $\tau^M(i)$ represents the set of nodes with a distance of M hops from node i. If the most central node in the network is mined, the shortest path between nodes is the shortest path based on transmission delay; if the most stable data distribution node in the network is mined,

the shortest path between nodes is the shortest path based on social connections. M is the maximum number of hops, and the specific value can be set according to the actual application requirements.

Since the topology of opportunistic networks changes dynamically, human social connections are more permanent and stable than the topology of networks. Mining the social connections between nodes is of great significance to divide the opportunistic network into a more stable community structure [7]. Using the social connection index as a method to detect the social connection between routing nodes, the calculation formula is

$$\begin{cases} \lambda(i,j) = (N(i,j))^{\varepsilon(i,j)} \\ \varepsilon(i,j) = \frac{|\tau(i) \cap \tau(j)|}{\min\{|\tau(i)|, |\tau(j)|\}} \end{cases} \tag{7}$$

In formula (7), $\lambda(i,j)$ represents the social connection index of routing nodes; $N(i,j)$ represents the number of encounters between routing nodes i and j; $\varepsilon(i,j)$ represents the similarity between routing nodes i and j; $\tau(i)$ and $\tau(j)$ represent is the number of members in the neighbor set of routing node i and j.

Based on the global entropy centrality measure and social connectivity index, a publish-subscribe system is constructed for opportunistic networks. Firstly, the network is divided into communities based on the social connection index, and different communities are divided according to the closeness of the relationship between nodes. Regarding the selection of proxy nodes, the global entropy centrality measurement method is used to select the node with the largest global entropy centrality in each community as the proxy node to help other nodes in the community publish or subscribe event messages. Within a community, nodes submit event messages that need to be published or subscribed to proxy nodes; among communities, through the interaction between proxy nodes, the sharing of published event messages in the network is realized.

The routing node data publishing/subscribing rules are shown in Fig. 4.

As shown in Fig. 4, blue circles represent proxy nodes, and white circles represent neighbor routing nodes. Based on the publish/subscribe rules constructed above, a routing algorithm is proposed. Each node obtains the member information of its own community according to the community division algorithm based on social attributes, and selects the proxy node in the community according to the global entropy centrality measurement method. If there is a node in the network that does not belong to any community, and the node also needs to publish or subscribe event messages, assign the node to a default community. Each node in the community records the proxy node of the community to which it belongs. Proxy nodes need to dynamically maintain the relevant information of proxy nodes of other communities in the network [8].

Define the proxy node i of the community that node i belongs to as aaaaaaaaa a, when node i subscribes to proxy node a, if node meets node j, if node j is proxy node a, send the subscription message to node j; if node j is not a proxy The node a, and the local centrality $K(j)$ of the node j is greater than the local centrality $K(i)$ of the node i, and forwards the subscription message to the relay node j.

The detailed process of node i subscribing to proxy node a is as follows: when node i publishes a message to proxy node a, if node j is proxy node a, it will send the message to be published to node j; if node j is not proxy node a, At the same time, the local

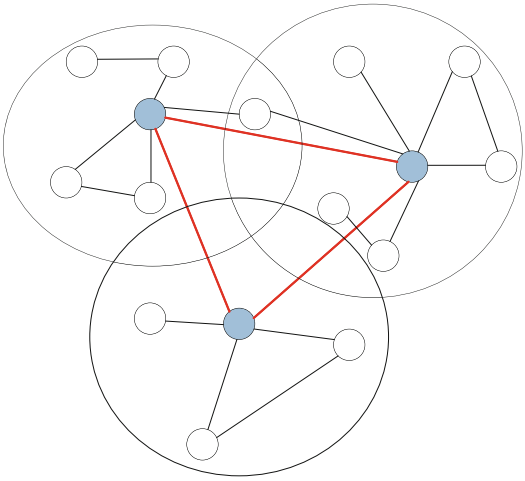

Fig. 4. Schematic diagram of routing node data publishing/subscription rules

centrality $K(j)$ of the node j is greater than the local centrality $K(i)$ of the node Z, and the message to be published is forwarded to the relay node j.

The detailed process of node i publishing a message to the proxy node a is: when the proxy node a receives the message that needs to be published, if the proxy node a meets the node k of other communities; if the node k is the proxy node of other communities, it will need to publish the message The message is forwarded to the node k; if the node k is not a proxy node of other communities, and the global entropy centrality $\gamma(k)$ of the node k k is greater than the global entropy centrality $\gamma(a)$ of the node a, send the message to be published to k, and continue to send the message through the node k Proliferate other proxy nodes.

The detailed process of sharing and publishing messages between proxy nodes is as follows: the proxy node a receives a message published by other communities, and if the message is a message subscribed by members in the community, it will spread the message in the community.

The detailed process of the proxy node publishing messages to the community is as follows: Since the topology of the opportunistic network changes dynamically, when a new node joins the community, the newly joined node sends a joining notification to the proxy node; if the proxy node in the community changes, the old proxy node transfers the subscription list of event messages in the community to the new proxy node, and the new proxy node sends the proxy change notification to the nodes in the community and the proxy nodes of other communities.

The above process completes the formulation of routing node data publishing/subscription rules, and expounds the detailed process of routing node data publishing/subscription, laying a solid foundation for the realization of final data security sharing.

2.4 Construction and Implementation of Data Security Sharing Architecture

Based on the routing node data publishing/subscription rules formulated above, combined with secure multi-party computing big data, a routing node data security sharing architecture is built, so as to realize the safe sharing of routing node data in opportunistic networks.

The routing node data security sharing architecture constructed in this research introduces secure multi-party computing big data into data sharing. An excellent sharing strategy can effectively protect the privacy of data. The main task of the data security sharing architecture based on secure multi-party computing big data is to atomize the secure multi-party computing big data, which is more convenient for data invocation, and can better be invoked by the integrated control module to provide interfaces for upper-layer applications [9].

The routing node data security sharing architecture is designed with a layered structure. The entire architecture is divided into three layers. The bottom layer is the data provider layer, the middle layer is the core computing layer, and the upper layer is the application layer. The data provider layer receives the data input by the routing node; the work to be done by the computing layer is to atomize various protocols and algorithms for secure multi-party computation, and then uniformly control these atomic operations to provide interfaces to the upper-layer applications. The upper layer is the application layer, which shows the data sharing process between routing nodes.

Although the routing nodes of the secure multi-party computation are all equal, due to the large amount of data computation involved in the secure multi-party computation, a semi-centralized node is proposed to simplify the computation, which is different from the ordinary central node. It is not trustworthy, and the information it receives is not real information, but only part of the steps of secure multi-party computing, and it is impossible to derive private information based on relevant information.

In addition, the internal structure of each routing node is basically the same, because of the equality of status, they need to complete the same functional steps in the process of secure multi-party calculation to obtain the final calculation result. The interior of the routing node is divided into a three-layer structure, the most important and the core of the secure multi-party computing data sharing model is the intermediate computing layer. This layer contains some protocols and algorithms for secure multi-party computation. Contains the operation elements of their secret sharing, and completes secure multi-party computation by means of polynomial interpolation. It also includes a secure matrix product operation element, and completes the secure two-party matrix product calculation by implementing a secure two-party protocol. At the same time, it also includes a secure comparison protocol, a simple secure summation protocol, and an inadvertent transfer protocol. The computing layer atomically operationalizes these secure multi-party computing protocol processes, and uses a hanging module for unified management to provide interfaces to the upper layer. In addition, this computing layer also includes the most important auxiliary module in the whole computing system: the communication module [10–12]. This module is an asynchronous communication module implemented with python twist. Any secure multi-party computing operation

is inseparable from this auxiliary module, and all interactions between nodes are completed through this module. The basic hierarchical structure of a single routing node is shown in Fig. 5.

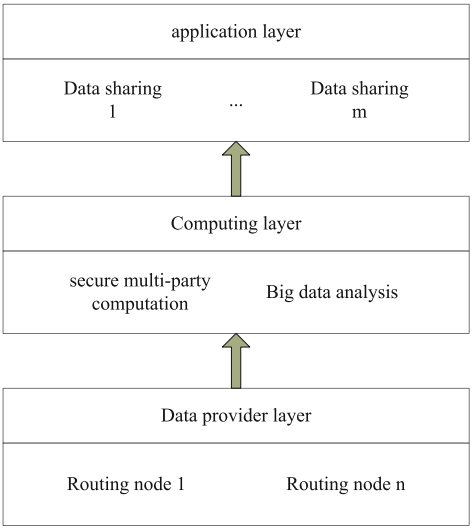

Fig. 5. Schematic diagram of the basic hierarchical structure of a single routing node

Secure multi-party computation is mainly to perform multi-party computation on the security of the data sharing process. The calculation formula is:

$$\begin{cases} \eta = \dfrac{\sum\limits_{i,j=1}^{n} \omega_{ij} Y_{ij}}{3\zeta_0} \\ \mu = 4\upsilon^* \cdot \sum\limits_{i,j=1}^{n} Y_{ij} \\ \vartheta = 9\hat{\kappa} \cdot \sum\limits_{i,j=1}^{n} \omega_{ij} Y_{ij} \end{cases} \tag{8}$$

In formula (8), η, μ and ϑ represent the security values corresponding to the data provider, the routing node and the data receiver during the data sharing process; ω_{ij} represents the weight coefficient corresponding to Y_{ij}; Y_{ij} represents the The path between routing nodes i and j; ζ_0 represents the auxiliary calculation parameter; υ^* represents the number of routing nodes; $\hat{\kappa}$ represents the amount of data required by the data receiver.

In order to facilitate the research, the secure multi-party calculation results are fused, and the expression is

$$\xi = \Phi_1 \eta + \Phi_2 \mu + \Phi_3 \vartheta \tag{9}$$

In formula (9), ξ represents the security value of the routing node data sharing process; Φ_1, Φ_2 and Φ_3 represent the weight coefficients corresponding to η, μ and ϑ.

Based on the calculation result of formula (9), the data sharing path selection rule is formulated as

$$\begin{cases} \xi \geq \sigma'' \text{ choose} \\ \xi < \sigma'' \text{ delete} \end{cases} \tag{10}$$

In formula (10), σ'' represents the security threshold of the routing node data sharing process.

Selecting the data sharing path to perform the data sharing operation according to the above can realize the secure sharing of the routing node data of the opportunistic network, and provide assistance for the development and application of the opportunistic network.

3 Experiment and Result Analysis

3.1 Experiment Preparation Stage

In order to verify the application performance of the proposed method, an opportunistic network in a certain area is selected as the experimental object. Since the routing nodes in the opportunistic network appear to be in a moving state, its structure cannot be displayed.MATLAB software was selected as the experimental platform, the hardware was configured as 3.20GHz CPU, 4.00GB memory, the software was configured as Windows7SP1 PC, and the operating environment was Visual Studio2010. Build the experimental environment on the MATLAB platform.

The proposed method applies several location parameters, which all affect the security of data sharing. Therefore, it is necessary to determine the optimal value of the parameters before the experiment. The experimental parameters are damping factor δ and auxiliary calculation parameter ζ_0.

The relationship between the damping factor δ and the calculation accuracy of the PageRank value Ψ_i of the influence degree of routing nodes is obtained through experiments, as shown in Table 1.

As shown in the data in Table 1, when the damping factor δ is 0.40, the calculation accuracy of the PageRank value Ψ_i of the routing node influence degree reaches the maximum value of 98%. Therefore, the optimal value of damping factor δ is determined to be 0.40.

The relationship between the auxiliary calculation parameter ζ_0 obtained through experiments and the accuracy of secure multi-party calculation is shown in Fig. 6.

As shown in the data in Fig. 6, when the value of the auxiliary calculation parameter ζ_0 is 0.3, the accuracy of the secure multi-party calculation reaches the maximum value of 90%. Therefore, it is determined that the optimal value of the auxiliary calculation parameter ζ_0 is 0.3.

The above process provides convenience for the subsequent experiments of data security sharing of opportunistic network routing nodes.

Table 1. The relationship between damping factor and calculation accuracy of PageRank value

δ	Ψ_i	δ	Ψ_i
0.05	85%	0.55	90%
0.10	75%	0.60	75%
0.15	71%	0.65	84%
0.20	68%	0.70	86%
0.25	85%	0.75	77%
0.30	80%	0.80	86%
0.35	71%	0.85	89%
0.40	98%	0.90	61%
0.45	92%	0.95	54%
0.50	92%	1.00	50%

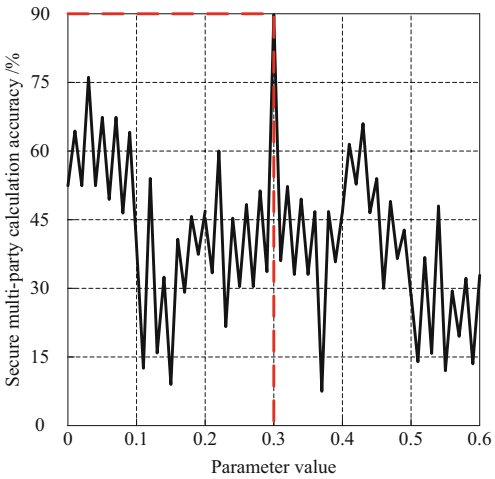

Fig. 6. Relationship between auxiliary calculation parameters ζ_0 and security multi-party calculation accuracy

3.2 Analysis of Experimental Results

In order to clearly show the application performance of the proposed method, the shared data packet loss rate and the data sharing safety factor are selected as evaluation indicators, and the calculation formula is:

$$\begin{cases} \Gamma_f = \frac{R_d}{R_{total}} \times 100\% \\ \Gamma_g = \forall sign(\xi)/\varphi_0 \end{cases} \tag{11}$$

In formula (11), Γ_f and Γ_g represent the shared data packet loss rate and data sharing safety factor; R_d and R_{total} represent the amount of lost data and the total amount of shared data; φ_0 represents the data sharing security conversion factor.

Based on the calculation formula of formula (11), the shared data packet loss rate obtained through experiments is shown in Fig. 7.

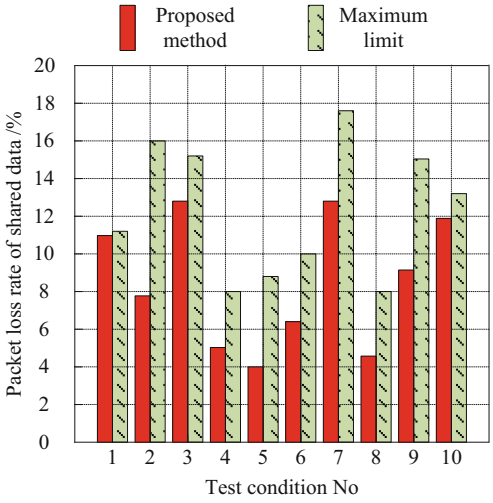

Fig. 7. Shared data packet loss rate data graph

As shown in Fig. 7, the shared data packet loss rate obtained by applying the proposed method is less than the maximum limit, and the minimum value is 4%.

The method of reference [1] and the method of reference [2] are compared.The safety factor of data sharing obtained through experiments is shown in Table 2.

As shown in the data in Table 2, the data sharing safety factors obtained by the proposed method are all larger than the minimum limit, and the maximum value is 0.98.The data sharing safety coefficient of the two literature methods is less than 0.70, and part of it is less than the minimum limit.

The above experimental results show that after the proposed method is applied, the packet loss rate of shared data is less than the maximum limit, and the safety factor of data sharing is greater than the minimum limit, which fully confirms the effectiveness and feasibility of the proposed method.This is because the method in this paper establishes the influence propagation model of routing nodes, establishes the data release/subscription rules of routing nodes, and combines the big data calculation of secure multi-parties to build the data security sharing architecture of routing nodes, so as to realize the security sharing of routing node data in opportunistic networks.

Table 2. Data sharing safety factor table

Experimental condition number	Suggested method	Method of literature [1]	Method of literature [2]	Minimum limit
1	0.84	0.46	0.44	0.45
2	0.76	0.55	0.55	0.56
3	0.89	0.62	0.61	0.62
4	0.90	0.61	0.60	0.61
5	0.91	0.58	0.63	0.59
6	0.92	0.50	0.51	0.50
7	0.90	0.64	0.62	0.60
8	0.84	0.67	0.65	0.67
9	0.86	0.62	0.64	0.63
10	0.98	0.69	0.68	0.70

4 Conclusion

This research introduces the knowledge graph theory and big data technology, and proposes a new method for data security sharing of opportunistic network routing nodes, and also provide some help for the application and development of the Opportunity Network.

References

1. Fatima, S., Ahmad, S.: Secure and effective key management using secret sharing schemes in cloud computing. Int. J. e-Collaboration **16**(1), 1–15 (2020)
2. Yang, J., Wen, J., Jiang, B., et al.: Blockchain-based sharing and tamper-proof framework of big data networking. IEEE Network **34**(4), 62–67 (2020)
3. Hassija, V., Chamola, V., Garg, S., et al.: A blockchain-based framework for lightweight data sharing and energy trading in V2G network. IEEE Trans. Veh. Technol.Veh. Technol. **69**(6), 5799–5812 (2020)
4. Dang, Q., Ma, H., Liu, Z., et al.: Secure and efficient client-side data deduplication with public auditing in cloud storage. Int. J. Network Secur. **22**(3), 462–475 (2020)
5. Chen, Y., Hu, B., Yu, H., et al.: A threshold proxy re-encryption scheme for secure IoT data sharing based on blockchain. Electronics **10**(19), 2359 (2021)
6. Liu, Q., Zhang, W., Ding, S., et al.: Novel secure group data exchange protocol in smart home with physical layer network coding. Sensors **20**(4), 1138 (2020)
7. Yue-bo, L., Wei-jie, Z.: Implementation of dynamic clustering scheduling algorithm for social network data. Comput. Simul. **38**(1), 269–272 (2021)
8. Zhang, Z., Ren, X.: Data security sharing method based on CP-ABE and blockchain. J. Intell. Fuzzy Syst. Appl. Eng. Technol. **2**, 40 (2021)
9. Tan, H.-C., Soh, K.L., Wong, W.P., Tseng, M.-L.: Enhancing supply chain resilience by counteracting the achilles heel of information sharing. J. Enterp. Inf. Manage. **35**(3), 817–846 (2022). https://doi.org/10.1108/JEIM-09-2020-0363

10. Jibb, L., Amoako, E., Heisey, M., et al.: Data handling practices and commercial features of apps related to children: a scoping review of content analyses. Arch. Dis. Child. **7**, 107 (2022)
11. Sharma, N., Anand, A., Singh, A.K.: Bio-signal data sharing security through watermarking: a technical survey. Computing: Archives for informatics and numerical computation **103**(9), 1883–1917 (2021)
12. Singh, C., Sunitha, C.A.: Chaotic and Paillier secure image data sharing based on blockchain and cloud security. Expert Syst. Appl. **198**, 116874 (2022)