Hindawi
Security and Communication Networks
Volume 2022, Article ID 6343764, 12 pages
https://doi.org/10.1155/2022/6343764

Research Article

A Hybrid Opportunistic IoT Secure Routing Strategy Based on Node Intimacy and Trust Value

Lin Yu,[1,2] **Gang Xu**,[1,2] **ZhiFei Wang**,[1,2] **Na Zhang**,[1,2] **and FengQi Wei**[1,2]

[1]*College of Computer Science, Inner Mongolia University, Hohhot 010021, China*
[2]*Inner Mongolia A.R. Key Laboratory of Data Mining and Knowledge Engineering, Inner Mongolia University, Hohhot 010021, China*

Correspondence should be addressed to Gang Xu; csxugang@imu.edu.cn

Received 11 July 2021; Revised 4 December 2021; Accepted 13 January 2022; Published 9 February 2022

Academic Editor: Qi Jiang

Routing strategy is one of the most important researches in Opportunistic Internet of Things (IoT), and it highly influences the efficiency of data transmission. In this paper, a hybrid Opportunistic IoT secure routing strategy based on node intimacy and trust value (HIRouter) is proposed to resolve the problem of unbalanced transmission efficiency and security in the message delivery process. According to the records of node encounter and message forwarding, the strategy proposed in this paper can calculate nodes' intimacy and trust value. The messages are then forwarded based on the intimacy and trust value between nodes. Experimental results verify that HIRouter algorithm we proposed can improve the message delivery rates and reduce the overhead rate in the Opportunistic IoT with dense nodes and frequent interactions between nodes.

1. Introduction

IoT is a network that uses sensing devices to connect objects and networks and enable objects to interact and exchange information, then achieve intelligent identification and management. It is mainly used in fields such as intelligent transportation, intelligent logistics, and smart cities. Opportunistic IoT is a kind of information interactive IoT characterized by temporary, opportunistic, and mobile self-organization. Opportunistic IoT enables intelligent objects to interact with each other by contact opportunity during the node moving [1–3]. Figure 1 shows an application scenario of the opportunistic IoT. An opportunistic network is derived from the delay-tolerant network [4–7]. There are no specific links between nodes in opportunistic networks, and messages are propagated in a "store-carry-forward" manner [8–10]. Research hotspots related to opportunistic networks include routing strategies, congestion control [11–14], energy consumption [15–18], and incentive mechanisms [19–23]. Among these, routing strategies are the key points of opportunistic network research. Currently, several routing algorithms have been proposed. The most prominent routing algorithm is the epidemic algorithm. In the algorithm, nodes can forward their information to every node they encounter in the network before reaching the destination node [24]. The node of the spray and wait (S&W) algorithm produces L message copies for L neighboring nodes; then the L nodes that receive the copies seek the destination node [25–28]. The PROPHET algorithm forwards messages based on the historical information of node encounters 29.

Messages are forwarded in a "storage-carry-forward" manner in mobile Opportunistic IoT; in other words, messages are placed in intermediate node buffers [30]. Data transmission and distribution are completed through the encounter and contact opportunities created by node movements, and data eventually reach the destination node. The performance related to forwarding basis, such as message delivery success rate, transmission latency, and network resource consumption, determine the efficiency of message transmission in the data transmission process. Using the historical encounter information between nodes, the PROPHET routing algorithm formulates message-forwarding strategies; however, updating the message-

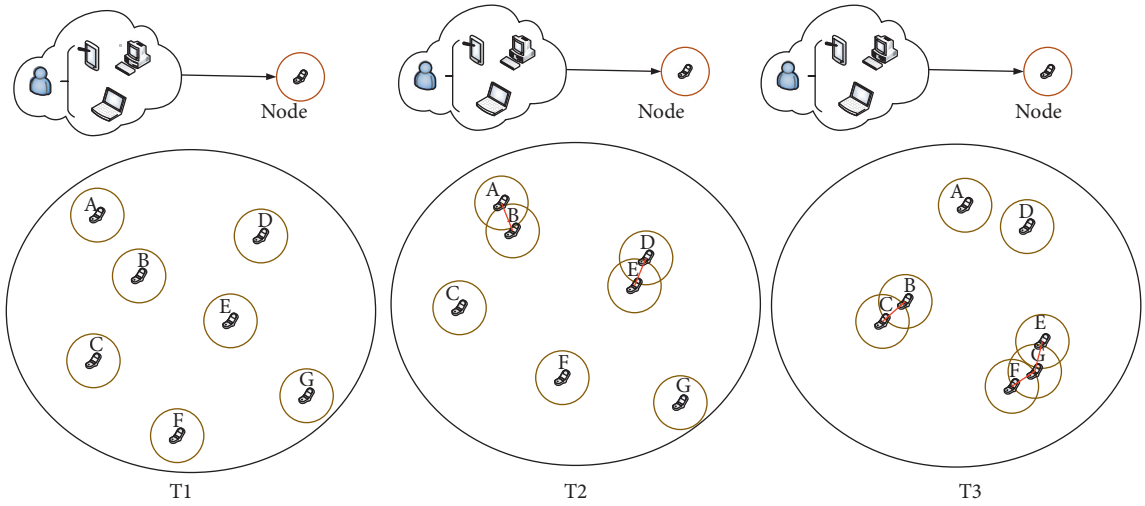

Figure 1: IoT application scenario.

forwarding efficiency in real-time with changes in the operating environment is difficult. A trusted routing scheme based on social similarity (TRSS) incorporates social trust into the routing decision process [31]. In the TRSS scheme, nodes move and associate with each other based on their common interests or social similarities and the next-hop forwarding node is assumed to be the node exhibiting common social characteristics with the destination node. This scheme mainly targets untrustworthy nodes, i.e., greedy or malicious nodes. The schema is not universal. In this paper, a hybrid Opportunistic IoT secure routing strategy based on node intimacy and trust value is proposed. The mixed utility value of node intimacy and trust value is determined by the historical data information of nodes and successful message-forwarding records. Moreover, messages are forwarded from nodes with low mixed utility values to nodes with high mixed utility values until the destination node is reached. The probability of messages being forwarded to selfish and malicious nodes is reduced, which laterally improves the security of messages in the network.

2. Related Works

Ma reviewed the research progress on mobile opportunistic network routing and described the main research content of mobile opportunistic networks in detail [9]. Li proposed a trust-based opportunistic routing (TOR) method by exploiting the trust mechanism, which improves the forwarding efficiency and information security of nodes in the opportunistic network [32]. The TOR method is suitable for networks with more malicious and greedy nodes. Although the bundling and carrying mechanism of the method improves security, it also increases the information storage consumption under this mechanism.

In order to solve the problem that the selfishness of the node due to the energy consumption of the message transmission leads to the serious degradation of the message transmission process and the increase of the network delay, N. Gupta proposed an incentive design mechanism based on contract theory to reward intermediate nodes appropriately to forward the messages [30]. This mechanism appropriately encourages intermediate nodes to forward messages. According to their ability to forward the message, the mechanism divides nodes into a finite number of types and model the service transaction between the forwarding node and the forwarding node. The necessary and sufficient conditions are further derived to provide incentives for nodes participating in message forwarding so that the nodes are more active in the process of message transmission.

Based on the temporal and spatial constraints of node movement in a social-based opportunistic network, Yao proposed an energy-efficient message-forwarding algorithm in community-based opportunistic networks [33]. The algorithm divides the nodes in the network into communities and uses different transmission strategies for intra-community and intercommunity. The algorithm balances the efficiency of data forwarding on the opportunistic network with the energy consumption of the network. However, high message-forwarding efficiency cannot be achieved using this algorithm.

Based on the connection time, Duan proposed a probabilistic routing algorithm named PROPHET-CT, which resolved the problem of heavy network loads when the PROPHET routing algorithm calculated the node encounter probability [34]. The algorithm achieves a high message delivery success rate in the node-intensive scenario, but the delivery success rate is lower in a network with sparse nodes.

A trust-based data forwarding algorithm was proposed by Yuan [35]. The node trust value is determined by the three social attributes, and messages are forwarded in the network based on the trust value. However, this algorithm does not consider the influence of the message-forwarding path on the node trust value and the subsequent effect on the forwarding efficiency.

Since nodes in opportunistic networks have a large autonomy, there are many nodes that exhibit selfishness or even malicious behavior. For these nodes, Liu proposed an

alert system for bins based on opportunistic networks [36]. The system primarily evaluates whether the nodes are trustworthy for information transmission and forwards the message to the trusted nodes. This system is only applicable to networks in which the nodes have greater node autonomy and are not universal.

For the problem of inefficient message transmission due to unreliable link quality between nodes in the network, Yang proposed an opportunistic routing algorithm based on node connectivity [37]. The algorithm defines a set of forwarding candidates and the priority of each candidate node ensures efficient data transmission and reduces energy consumption during data transmission. The algorithm determines the reliability between nodes only based on node connectivity, which is always slightly incomplete, and the relationship between nodes should be fully considered.

Since the independence maintained by nodes in the process of motion will have a certain impact on data transmission, Zhang proposed an opportunistic network routing algorithm based on node motion for the motion characteristics of nodes [38]. The algorithm's data forwarding priority evaluation model and differential copy transfer policy guarantee message group delivery and lower delivery latency while limiting system overhead. The algorithm does not achieve a high delivery rate in networks with sparse nodes, so the algorithm is only suitable for networks with a certain node density.

A routing strategy for ad hoc networks based on node degree estimation and static game forwarding strategy is proposed for the broadcast storm problem caused by broadcast route grouping in the route discovery process of ad hoc networks [39]. The node degree estimation method and static game forwarding strategy of the strategy greatly reduce the network consumption caused by broadcasting Hello messages to obtain node degree information and also reduce a large amount of redundancy, competition, and conflicts generated during the route request packet broadcasting process, and improve the efficiency of route request packet broadcasting in the route discovery process. The strategy is currently only applicable to scenarios where the number of network nodes is large, and the nodes are evenly distributed in the network.

To address unreliable transmission in the network, Prashant Kumar proposed a reliability strategy [40]. In this strategy, the source node can recognize the message status. If an error in message transmission occurs, the source node can respond appropriately to resend the message. The strategy is instrumental because even if a message is lost, the message-forwarding success rate will not decrease.

T. Spyropoulos proposed an efficient routing scheme for intermittently connected mobile networks (S&W) [28]. S&W routing is divided into two phases, the node distributes the message to their neighbor nodes during the spraying phase, and the waiting phase carries the message nodes to the destination node. This scheme controls the number of copies of the message to be delivered in the network and solves the disadvantages of contagion routing. In the scheme, the control of the number of copies of messages is a very important issue.

In order to solve the problem of how to transmit messages when there is no linking path between the source node and the destination node, A Vahdat proposed epidemic routing for partially connected ad hoc networks (epidemic) [41]. The nodes in this route deliver the messages to all the encounter nodes, so ideally the delivery rate of this algorithm is the highest as long as the cache of the node is large enough. This is an extreme situation. In fact, the size of the node buffer is not enough to receive all the messages from other nodes, so the delivery rate of this route is not high due to the cache problem.

Lindgren proposed probabilistic routing in intermittently connected networks (Prophet) [42]. Prophet routing uses the historical encounter information between nodes to dynamically update the predicted value of the node's delivery. The message is delivered according to the predicted delivery value. If the predicted delivery value of the encountering node is higher than the node currently carrying the message, the message is copied and forwarded. The route is more suitable in areas with high node density and frequent encounters and is not suitable for remote areas where nodes are sparse.

To solve the problem of uneven energy consumption of nodes due to excessive calculation of key nodes and the loss of important messages due to limited remaining cache of nodes, Chen proposed an energy balance and cache optimization routing algorithm based on communication willingness (EC_CW) [43]. Based on the PROPHET algorithm, this algorithm forwards messages according to the multicopy mechanism and the willingness to communicate between nodes. In a sparse node network environment, it reduces the average delay and overhead rate, and in a node dense network environment, it improves the delivery rate. Although the delivery rate of the algorithm has been improved, its delivery rate is still at a relatively low level.

In summary, the existing opportunistic network routing algorithms do not consider the forwarding efficiency when data security is guaranteed. To this end, a hybrid opportunistic IoT secure routing strategy based on node intimacy and the trust value is proposed. The routing strategy mainly calculates the mixed utility value between nodes based on the encounters between the nodes and the message-forwarding path. The mixed utility value is used as the basis for message forwarding. This strategy considers the encounter situations between the nodes and successful message-forwarding records to ensure that messages are forwarded to the nodes with high intimacy and trust value thereby the strategy balances the efficiency and security of data forwarding.

3. Intimacy

In this work, a double hash table is used to simulate the relevant information between nodes in a matrix, which is stored under each node. Then, the nodes update the hash table during moving. Thus, by storing information about all nodes under every single node, the concept of decentralization can be implemented. The contents stored in the double hash table are shown in Figure 2.

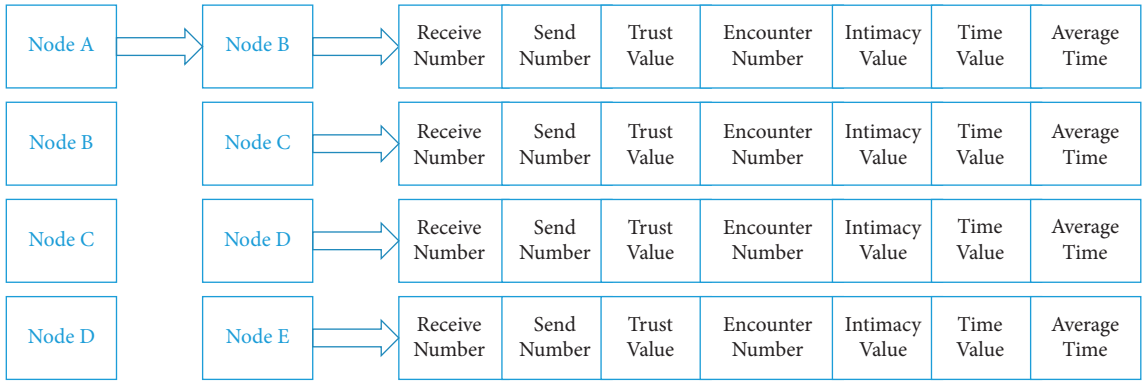

Figure 2: Information storage structure.

3.1. Encounter Information

Definition 1. EncounterNumber (EN) represents the number of connections between two nodes [44], i.e., the number of times two nodes have reached each other's communication range.

When two nodes are connected, each node updates its EncounterNumber information in the hash tables.

Definition 2. EncounterDuration (ED) represents the duration of node encounter [44], i.e., the length of time from when the communication link between two nodes is connected to when the communication link is disconnected.

Time Value indicates the connection time. The calculation of node encounter duration is shown as follows:

$$\text{EncounterDuration} = \text{CurrrentTime} - \text{TimeValue}. \quad (1)$$

Definition 3. AverageEncounterDuration (TI) denotes the average encounter duration of each encounter between nodes [44], i.e., the ratio of the total encounter duration to the number of encounters between two nodes during network operation.

Generally, if the node encounter duration is short, network bandwidth is small, or transmission data are large, then complete data delivery may not be guaranteed. Therefore, forwarding messages to nodes with a longer average encounter duration can more effectively improve the message-forwarding success rate. To avoid forwarding messages to nodes with a short meeting duration, we need to calculate the average encounter duration $TI_{(avg,i,j)}$ of the node. When two nodes are disconnected, the encounter time and average encounter duration between the two nodes are calculated and stored. The average encounter duration is calculated as shown below:

$$TI_{(avg,i,j)} = \frac{\sum_{k=1}^{n} TI_k}{n},\ k \le n. \quad (2)$$

TI_k is the duration of the kth encounter between node i and j, and $\sum_{k=1}^{n} TI_k$ represents the sum of n encounter time.

3.2. Intimacy Information

Definition 4. Intimacy Value (I) signifies the frequency of contact between nodes during network operation.

More closely related nodes will meet frequently, while less closely related nodes will meet with a low probability. The node intimacy can be calculated using their meeting information, as follows:

$$I_{(i,j)} = EN_{(i,j)} * w + TI_{(avg,i,j)} * (1 - w). \quad (3)$$

Let $I_{(i,j)}$ denote the intimacy between nodes i and j, let $EN_{(i,j)}$ denote the number of encountering nodes, and let $TI_{(avg,i,j)}$ denote the average encounter time between nodes i and j. The variable w represents a weight value, $0 < w < 1$; the w is determined to be 0.57 based on the ratio of the encounter duration and the number of encounters in the experiment.

4. Trust Degree

Definition 5. Trust degree (T) between the destination and current nodes is defined as the ability of the current node to forward messages to the destination node. Based on successful message-forwarding records, the trust reward of the node forwarding data to the destination node is calculated.

Based on the forwarding path of the node successfully forwarding the message to the destination node, the trust degree of the destination node to other nodes on the successful path is determined.

4.1. Forwarding Path.

In the simulation experiment, the messages are tracked, and the message-forwarding process is recorded. When the message successfully reaches the destination node, the successful message-forwarding path of this message is obtained.

Obtain the message-forwarding path:

$$\text{Path: } N_0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow N_4 \longrightarrow \ldots \longrightarrow N_j. \quad (4)$$

By obtaining the message-forwarding record, the nodes on the path on which the message is successfully forwarded are obtained, and these nodes are rewarded with trust.

To reflect the fairness and incentive of rewards for each node, a trust reward mechanism is established:

(1) The position of the forwarding node in path(N_i) determines the trust reward value of the forwarding node. If the forwarding node is closer to the destination node, the trust reward value of the forwarding node is higher, and vice versa. The trust reward value represents the trust degree between the destination and forwarding nodes and can be understood as the probability of the node forwarding a message to the destination node again in the future message-forwarding process.

(2) For messages with the same communication link length, a shorter message delay time Δt (reception time - creation time) signifies a greater trust reward value of the forwarding node. The smaller the Δt, the less time it will require for the forwarding node to transmit the message to the destination node, i.e., smaller delay.

4.2. Trust Reward. The currently rewarded node is provided with a trust value for the first time, as follows [32]:

$$T_{ij}^{(m)} = \frac{1}{2}\left(e^{-\lambda\times(\Delta t/TTL)} + \varphi + (1-\varphi)\times\left(\frac{\text{path}(N_i)}{|\text{path}(m)|}\right)^2\right). \quad (5)$$

$T_{ij}^{(m)}$ represents the trust reward value of node j to node i, and $e^{-\lambda\times(\Delta t/TTL)}$ represents the time reward function. The smaller Δt is (i.e., the less time it takes for the message to be received from the creation to the destination node), the greater the reward obtained. The value of $(\Delta t/TTL)$ ranges from 0 to 1, and λ is the message delay reward adjustment factor. $\varphi + (1-\varphi)\times(\text{path}(N_i)/|\text{path}(m)|)^2$ is the trust reward value function, which is determined according to the position of the node in the path, φ is the adjustment factor of trust reward value, $|\text{path}(m)|$ represents the length of the entire forwarding path, path(N_i) represents the position of node N_i in the forwarding path, and the value of path(N_i) is between 1 and $|\text{path}(m)|$, i.e., $(\text{path}(N_i)/|\text{path}(m)|)$ is between 0 and 1. In the trust mechanism, the closer the node position is to the destination node, the larger the path(N_i) is and the greater the trust reward value is obtained. The message is forwarded from a low-trust-value node to a high-trust-value node.

The old trust value of the currently rewarded node is shown in the following:

$$T_{ij}^{(m)} = \text{old Trust Value} + (1 - \text{old Trust Value})\times T_{ij}^{(m)}. \quad (6)$$

The trust value is updated based on the old trust value and the new reward trust value.

The node repeatedly forwards the message to the destination node and gradually improves the trust value reward; in this way, an oriented trust is established between the nodes in the network. Therefore, there is a trust-based forwarding mechanism in the network. The mechanism can be expressed as a two-dimensional array. The index of the array is the node address value, and the content of the array is the size of the trust value.

When the message reaches the destination node, the Δt of the message is calculated by obtaining message reception time and creation time. Then, the time reward function is calculated using Δt and time-to-live (TTL) of the message. The message transmission path and the trust table of the destination node are obtained, and the path is traversed. If a node does not have a trust record in the trust table of the destination node, the trust calculation using the formula (5) is performed.

5. A Hybrid Opportunistic IoT Routing Algorithm Based on Node Intimacy and Trust Value

In the message-forwarding routing process, the node considers the encounter information with other nodes and the trust value of the two encountering nodes under the destination node. When determining whether the message should be forwarded to the meeting node, the routing mechanism will assign weights to the two forwarding bases to calculate the final forwarding probability.

Because the storage structure uses a hash table, the node address value corresponds to the key value of the hash table, and the relevant information about the node corresponds to the value of the hash table. The algorithm directly obtains the value of the hash table based on the key value of the hash table; hence, the time complexity of the algorithm is $O(1)$.

Forwarding probability is the mixed utility value.

Definition 6. The mixed utility value (denoted by FB) is obtained by the weighted summation of the intimacy and trust value of the nodes. It is used to describe the reliability relationship between nodes. This value is calculated using formula equation (6):

$$FB = T_{il}^{(m)}\times\alpha + \frac{EN_{(i,l)}}{EN_{(i,l)} + EN_{(j,l)}}\times\beta + \frac{TI_{(\text{avg},i,l)}}{TI_{(\text{avg},i,l)} + TI_{(\text{avg},j,l)}}\times\gamma. \quad (7)$$

$EN_{(i,l)}$ is the number of encounters between the meeting node i and destination node l, $EN_{(j,l)}$ is the number of encounters between the current node j and destination node l, $TI_{(\text{avg},i,l)}$ is the average encounter duration between the meeting node i and destination node l, and $TI_{(\text{avg},j,l)}$ is the average encounter duration of the current node j and destination node l.

The forwarding probability calculation of the encounter node phase forwarding the message to the destination node consists of three parts: the trust degree of this encounter node under the destination node; the ratio of the number of encounters between the encountered node and the destination node and the number of encounters between the two nodes and the destination node respectively; the ratio of the encounter duration between the encountered node and the destination node and the sum of the encounter duration

(i) Input: Path, Trust Set(Node$_{\text{destination}}$)
(ii) Output: $T_{ij}^{(m)}$
(1) **While** message $->$ Node$_{\text{destination}}$ **do**
(2) Get Emulator Current Time
(3) Get Message Create Time
(4) Δt = Emulator Current Time − Message Create Time
(5) Get Δt, TTL
(6) $CalH = e^{-\lambda \times (\Delta t/TTL)}$
(7) Get Path, Trust Set(Node$_{\text{destination}}$)
(8) For $i \in$ Path do
(8) If Node(i)! = $NULL$ then
(9) $T_{ij}^{(m)}$ = old Trust Value + (1 − old Trust Value) × $T_{ij}^{(m)}$
(10) Else
(11) $T_{ij}^{(m)} = 1/2(H + \varphi + (1 - \varphi) \times (\text{path}(N_i)/|\text{path}(m)|)^2)$
(12) End If
(13) End For
(13) End While

Algorithm 1: Trust reward algorithm.

(i) Input: Trust Set(Node$_{\text{destination}}$)
(ii) Output: message forwarding
(1) **While** (connection Node$_A$, Node$_B$)
(2) If Node$_B$ == Node$_{\text{destination}}$
(3) message $->$ Node$_B$
(4) Else
(5) Get Trust Set(Node$_{\text{destination}}$)
(6) **If** Key(Node$_A$) ≠ NULL **then**
(7) Get Value(Node$_A$)
(8) End If
(9) If Key(Node$_B$) ≠ NULL then
(10) Get Value(Node$_B$)
(11) End If
(12) $Cal\, FB_{A,\text{destination}}, FB_{B,\text{destination}}$
(13) **If** ($FB_{B,\text{destination}} > FB_{A,\text{destination}}$) **then**
(14) message $->$ Node$_B$
(15) **Else**
(16) message $->$ Node$_A$
(17) End If
(18) End If
(19) End While

Algorithm 2: Message-forwarding algorithm.

between the two nodes respectively and the destination node. These three components are weighted and summed separately to obtain the forwarding probability of the encountered node. Similarly, the forwarding probability of the node currently carrying the message is also calculated in this way. α, β, and γ are the weights of the trust, the number of encounters, and the average duration of the encounters, respectively. The values of α, β, and γ are experimentally determined to be 0.1, 0.7, and 0.2, respectively. As shown in Figure 3, x, y, and z represent α, β, and γ, respectively. A more intense red color signifies a higher delivery success rate.

Step 1. indicates that the message-forwarding node meets the other nodes and establishes a connection. Steps 2–17 signify whether the currently established node performs message transmission. Steps 2–3 mean that if the message-forwarding node meets the destination node, the message is directly forwarded to the destination node. Steps 4–12 reflect that if the message-forwarding node does not meet the destination node, the node information is first obtained, and then the mixed utility value is calculated. Steps 13–16 indicate that if the mixed utility value of the message-forwarding node is less than that of the meeting node, the

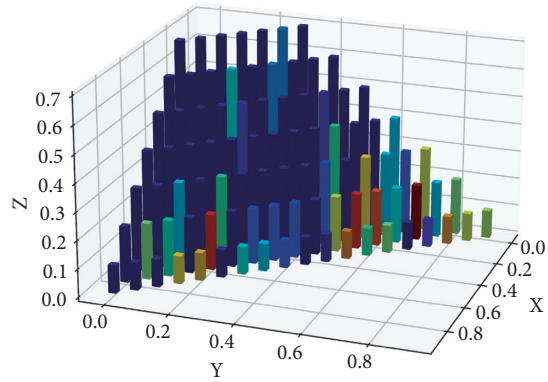

Figure 3: Success rates under different α, β, and γ.

message is forwarded to the meeting node; otherwise, it is not forwarded.

6. Experimental Environment and Configuration

The algorithm we proposed was experimentally verified, and performance analysis is conducted on the simulation tool ONE [45]. The simulation tool version 1.4.1 is used in the work. Table 1 shows the design of simulation experiment parameters.

6.1. Performance. Several indicators are often used to determine the performance of the network.

Herein, the five indicators used for network performance evaluation and the importance of the five indicators are listed below.

The delivery rate is undoubtedly the most important in Opportunistic IoT. The higher the delivery rate, the more messages successfully forwarded to the destination node. The second is the average delay and overhead rate. The less time the message is delivered in the network and the smaller the cache overhead of the nodes in the network, the better the performance of the network. Finally, the number of relay nodes and the average number of relay nodes. The smaller the number of relay nodes means that the fewer times the message is forwarded by the node in the network, the less the total energy consumed by the node to forward the message, and the more the network performance can be improved.

(1) Success rate is the ratio of the number of messages successfully forwarded to the destination node to the total number of messages. The indicator is denoted as equation (7).

$$S_{\text{success\_rate}} = \frac{N_{\text{delivered}}}{N_{\text{created}}}. \tag{8}$$

(2) Average hops are the average number of hops required for a message to be successfully forwarded to the destination node. The indicator is denoted as equation (8).

$$N_{\text{average\_hops}} = \frac{N_{\text{total\_hops}}}{N_{\text{delivered}}}. \tag{9}$$

(3) Number of relay nodes is the number of intermediate nodes required for the successful forwarding of a message to the destination node. The indicator is denoted as equation (9).

$$N_{\text{relay\_nodes}} = N_{\text{intermediate\_delivery\_nodes}}. \tag{10}$$

(4) *Average delay* is the average time required for a message to be forwarded from the forwarding node to the destination node. The indicator is denoted as equation (10).

$$N_{\text{average\_delay}} = \frac{N_{\text{total\_intermediate\_delivery\_nodes}}}{N_{\text{delivered}}}. \tag{11}$$

(5) Routing overhead is the ratio of the difference between the number of delayed messages and the number of successfully forwarded messages to the number of successfully forwarded messages. The indicator is denoted as equation (11).

$$R_{\text{overhead\_rate}} = \frac{N_{\text{relayed}} - N_{\text{delivered}}}{N_{\text{delivered}}}. \tag{12}$$

6.2. Experiment Analysis. In the experiment, by increasing the number of nodes in the network, the performance of HIRouter is compared with the performance of the epidemic [41], PROPHET [42], EC_CW [43], and S&W algorithms [28].

6.2.1. Success Rate. In Figure 4, when the number of nodes is small, the success rates of the four algorithms do not differ considerably. As the number of nodes increases, the success rate of HIRouter significantly increases. Moreover, as the number of nodes increases, the transmission success rate of the epidemic algorithm increases, and the prediction accuracy of the propagation probability of the PROPHET and EC_CW algorithms also improve. Therefore, the success rates of the epidemic and PROPHET algorithms are slightly

Table 1: The settings of simulation experiment parameters.

Parameter	Value
Experimental map	Helsinki map
Experimental area size	4.5 × 3.4 km (width × height)
Intra-area node movement model	Map-based shortest path movement model
Experimental simulation time	12 h (43200 s)
Number of nodes	36/66/96/126/156
Communication radius	10 m
Transfer speed	250 KB/s
Node moving speed	The first group: 0.5 ~ 1.5 m/s the second group: 2.7 ~ 13.9 m/s the third group: 0.5 ~ 1.5 m/s the fourth group: 7 ~ 10 m/s the fifth group: 7 ~ 10 m/s the sixth group: 7 ~ 10 m/s
Node cache size	Person: 5 M tram: 50 M
Transfer method	Person: Bluetooth interface tram: Bluetooth/high-speed interface
Message generation interval	25 ~ 35 s
Message size	500 kb–1 MB
Message life cycle	5 h

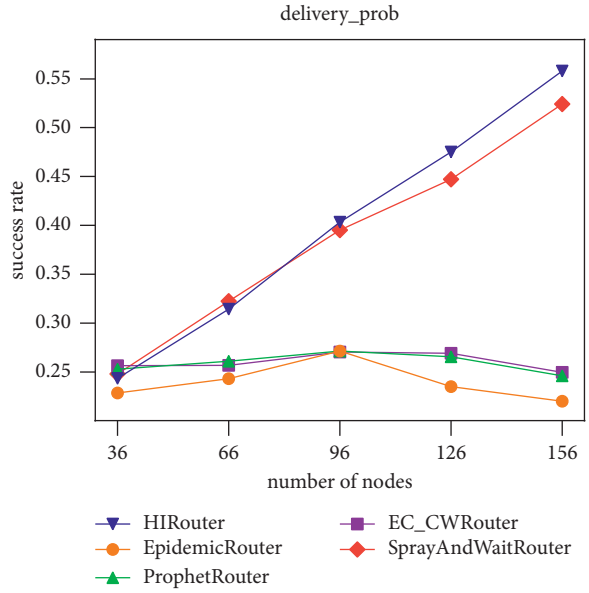

Figure 4: Success rate under the different number of nodes.

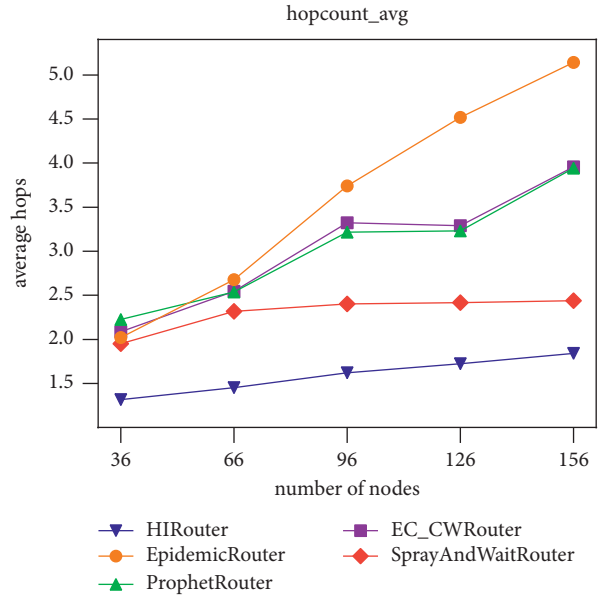

Figure 5: Average hops under the different number of nodes.

improved. The success rates of S&W and HIRouter algorithms are higher than those of the other two algorithms. Owing to an increase in the number of nodes in the S&W algorithm, the copy of spray's neighbor nodes significantly increases and the success rate also considerably increases. Compared with other routing algorithms, the HIRouter algorithm achieves the best success rate. As the number of mobile nodes increases, more accurate node relationships are estimated to provide a better forwarding strategy for opportunistic networks.

6.2.2. Average Hops. In Figure 5, as the number of nodes increases, the number of average hops of the epidemic algorithm increases, owing to the infection mechanism of the algorithm. Nodes will copy their message to forward it to the encountered nodes. The number of average hops of the PROPHET and EC_CW algorithms increases with the number of nodes; however, the increase is lower than that in the epidemic algorithm. The number of average hops of S&W and HIRouter algorithms slightly increases when the nodes are increased; however, the number of average hops of the HIRouter algorithm is relatively few. This finding demonstrates that the HIRouter algorithm selects the optimal relay nodes during message transmission, reduces the number of relay nodes, and ensures that the message reaches the destination node in as few hops as possible.

6.2.3. Number of Relay Nodes. In Figure 6, due to the contagion mechanism of the epidemic algorithm, the number of relay nodes increases with the number of nodes when the epidemic algorithm is used to transmit information. The PROPHET and EC_CW algorithms show an increased number of relay nodes when the number of nodes increases; however, the number of relay nodes is less than that in the epidemic algorithm. When the number of nodes

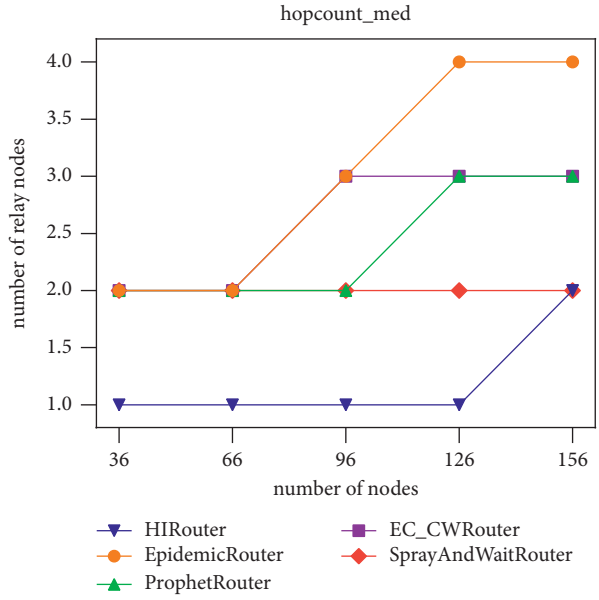

Figure 6: Number of relay nodes under different numbers of nodes.

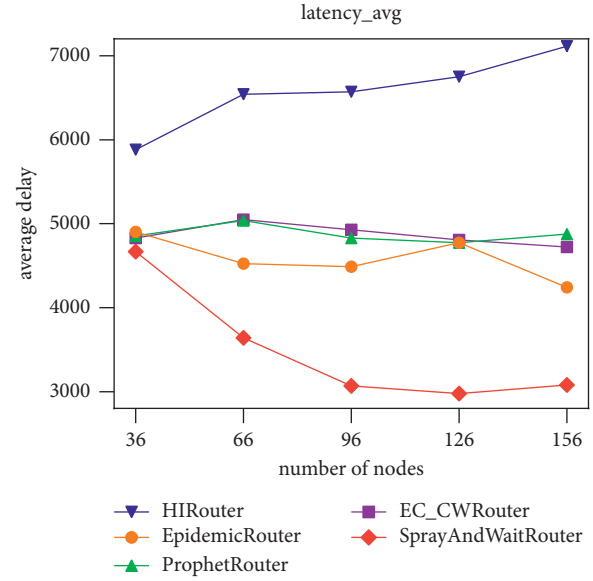

Figure 7: Average delay under the different number of nodes.

is small, the number of relay nodes of S&W and HIRouter algorithms is one. However, with an increasing number of nodes, the number of relay nodes of the HIRouter algorithm is minimal. This finding indicates that the HIRouter algorithm selects the optimal relay node during message transmission, thereby reducing the number of relay nodes; i.e., the number of message transmissions is reduced and the message loss rate is reduced.

6.2.4. Average Delay. In Figure 7, the average delay of the HIRouter algorithm is high. During message transmission, the nodes only forward messages to the nodes with a higher probability of transmission. In the procedure, the nodes may encounter many nodes that are not qualified for forwarding and wait for the relay nodes with a higher possibility of transmitting the message to the destination node or the destination node itself. Therefore, the average delay of the HIRouter algorithm is high.

6.2.5. Overhead Rate. In Figure 8, as the number of nodes increases, the overhead rate of the epidemic and PROPHET algorithm significantly increases. This is attributed to the infection mechanism of the epidemic algorithm. Messages are copied between the nodes that meet, and the memory

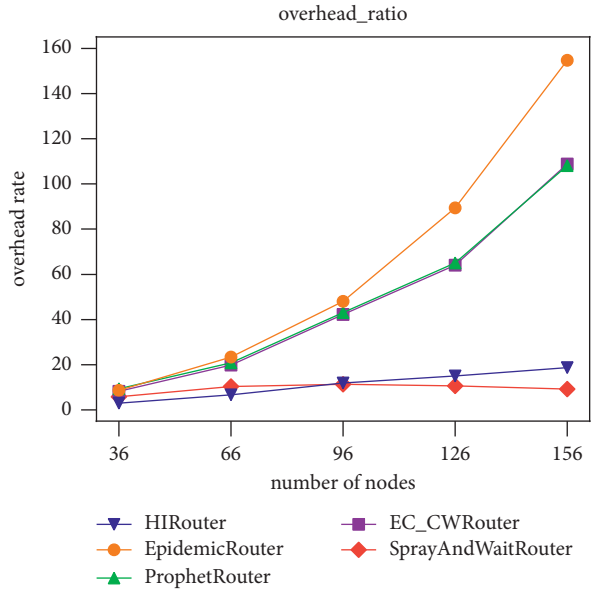

Figure 8: Overhead rate under the different number of nodes.

overhead is large. For the PROPHET and EC_CW algorithms, the recording of the forwarding probability and the calculation of the forwarding probability increase with an increasing number of nodes. Thus, the memory overhead increase. When the S&W algorithm is in the waiting phase, messages are forwarded only when nodes encounter the destination node, and there is no need for excess information recording and calculation. Therefore, as the number of nodes increases, the spray efficiency of the S&W algorithm shows no significant changes. As the number of nodes increases, although the overhead rate also increases, the HIRouter algorithm still maintains a low overhead. This is because the HIRouter algorithm selects better relay nodes when the message is forwarded, optimizing the delivery process and reducing overhead.

7. Conclusion

In this work, a hybrid Opportunistic IoT Secure routing strategy based on node intimacy and trust value is proposed. This strategy fully utilized the movement encounter information and successful message-forwarding information of the nodes in the network to determine the mixed utility value of nodes and identify the optimal relay nodes for message transmission.

From the experimental results, the HIRouter algorithm we proposed achieved a better success rate, a number of relay nodes, the average number of hops, and an overhead rate than the epidemic, PROPHET, EC_CW, and S&W algorithms. The routing algorithm improved the message delivery success rate and decreased the number of relay nodes and the average number of hops required for message transmission in the Opportunistic IoT with dense nodes and frequent interactions between nodes. At the same time, the routing algorithm reduces the information loss rate and the probability of malicious node damage from the side and improves the security of the network. Moreover, the routing algorithm decreases network congestion and resource consumption.

In summary, the HIRouter algorithm we proposed can effectively accomplish data transmission in Opportunistic IoT with high efficiency and quality. Although the HIRouter proposed in this paper has achieved certain results in terms of success rate and overhead rate, the routing algorithm has a high average delay, which has an impact on the network performance of opportunistic IoT. The algorithm determines the forwarding utility value through the encounter between nodes and the successful forwarding record of the message. Therefore, the algorithm is suitable for the Opportunistic IoT with dense nodes and frequent interactions between nodes. For the Opportunistic IoT with sparse nodes and less interaction between nodes, this algorithm does not have a better delivery efficiency. In future research, certain replica strategies and incentive mechanisms will be used to promote message forwarding to reduce the average delay and improve network performance and propose an algorithm for the Opportunistic IoT with sparse nodes and less interaction between nodes.

Data Availability

Data are available upon request.

Conflicts of Interest

The authors declare no conflicts of interest related to this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China under Grants 62061036, 61841109, and 62077032; Natural Science Foundation of Inner Mongolia

under Grant 2019MS06031 and in part by the Self-Open Project of Engineering Research Center of Ecological Big Data, Ministry of Education.

References

[1] A. Lohachab and A. Jangra, "Opportunistic Internet of Things (IoT): Demystifying the Effective Possibilities of Opportunisitc Networks towards IoT," in *Proceedings of the 2019 6th International Conference On Signal Processing And Integrated Networks (SPIN)*, pp. 1100–1105, Noida, India, March 2019.

[2] V. Petrov, A. Samuylov, V. Begishev et al., "Vehicle-based relay assistance for opportunistic crowdsensing over narrowband IoT (NB-IoT)," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3710–3723, 2018.

[3] M. Gharbieh, H. ElSawy, M. Emara, H.-C. Yang, and M.-S. Alouini, "Grant-free opportunistic uplink transmission in wireless-powered IoT: a spatio-temporal model," *IEEE Transactions on Communications*, vol. 69, no. 2, pp. 991–1006, 2021.

[4] Y.-P. Xiong, L.-M. Sun, J.-W. Niu, and Y. Liu, "Opportunistic networks," *Journal of Software*, vol. 20, no. 1, pp. 124–137, 2009.

[5] J. Sweta and C. Meenu, "Survey of buffer management policies for delay tolerant networks," *Journal of Engineering*, vol. 7, no. 3, pp. 117–123, 2014.

[6] C. Wang, D. Wang, G. Xu, and D. He, "Efficient privacy-preserving user authentication scheme with forward secrecy for industry 4.0," *Science China Information Sciences*, vol. 65, no. 1, 2022.

[7] P. Asuquo, H. Cruickshank, Z. Sun, and G. Chandrasekaran, "Analysis of dos attacks in delay tolerant networks for emergency evacuation," in *Proceedings of the 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, pp. 228–233, Cambridge, UK, September 2015.

[8] H. C. Gao, X. J. Chen, D. Xu, Y. Peng, Z. Y. Tang, and D. Y. Fang, "Balance of energy and delay opportunistic routing protocol for passive sensing network," *Journal of Software*, vol. 30, no. 8, pp. 2528–2544, 2019.

[9] H. D. Ma, P. Y. Yuan, and D. Zhao, "Research progress on routing problem in mobile opportunistic networks," *Journal of Software*, vol. 26, no. 3, pp. 600–616, 2015.

[10] Y. Lu, W. Wang, L. Chen, Z. Zhang, and A. Huang, "Opportunistic forwarding in energy harvesting mobile delay tolerant networks," in *Proceedings of the 2014 IEEE International Conference on Communications (ICC)*, pp. 526–531, Sydney, NSW, Australia, June 2014.

[11] J. Wu and Z. Chen, "Sensor communication area and node extend routing algorithm in opportunistic networks," *Peer-to-Peer Networking and Applications*, vol. 11, no. 1, pp. 90–100, 2018.

[12] M. Misumi and N. Kamiyama, "Evacuation-route recommendation using DTN with evacuee attributes in disasters," in *Proceedings of the2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, Nanjing, China, March 2021.

[13] S. Qiu, D. Wang, G. Xu, and S. Kumari, "Practical and provably secure three-factor Authentication protocol based on extended chaotic-maps for mobile lightweight devices," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, 2020.

[14] A. Marandi, M. Faghih Imani, and K. Salamatian, "Practical bloom filter based epidemic forwarding and congestion control in dtns: a comparative analysis," *Computer Communications*, vol. 48, pp. 98–110, 2014.

[15] F. De Rango and S. Amelio, "Geographic and energy aware epidemic strategy for mobile opportunistic DTN," in *Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–8, Honolulu, HI, USA, August 2020.

[16] A. Khalil, N. Mbarek, and O. Togni, "Fuzzy Logic based model for self-optimizing energy consumption in IoT environment," in *Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, Nanjing, China, March 2021.

[17] H.-T. Ye, X. Kang, J. Joung, and Y.-C. Liang, "Optimization for wireless-powered IoT networks enabled by an energy-limited UAV under practical energy consumption model," *IEEE Wireless Communications Letters*, vol. 10, no. 3, pp. 567–571, 2021.

[18] X. Zhou, X. Yang, J. Ma, and K. I.-K. Wang, "Energy efficient smart routing based on link correlation mining for wireless edge computing in IoT," *IEEE Internet of Things Journal*, vol. 1, 2021.

[19] G. Goudar and S. Batabyal, "Optimizing bulk transfer size and scheduling for efficient buffer management in mobile opportunistic networks," *IEEE Transactions on Mobile Computing*, vol. 1, 2021.

[20] J. Xu, J. Xiang, and D. Yang, "Incentive mechanisms for time window dependent tasks in mobile crowdsensing," *IEEE Transactions on Wireless Communications*, vol. 14, no. 11, pp. 6353–6364, 2015.

[21] S. K. Dhurandher, J. Singh, M. S. Obaidat, I. Woungang, S. Srivastava, and J. J. P. C. Rodrigues, "Reinforcement learning-based routing protocol for opportunistic networks," in *Proceedings of the ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, Dublin, Ireland, June 2020.

[22] D. Wang, X. Zhang, Z. Zhang, and P. Wang, "Understanding security failures of multi-factor Authentication schemes for multi-server environments," *Computers & Security*, vol. 88, no. 2020, pp. 1–13, 2020.

[23] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 8, pp. 6692–6702, 2015.

[24] R. Ramanathan, R. Hansen, P. Basu, R. Rosales-Hain, and R. Krishnan, "Prioritized epidemic routing for opportunistic networks," in *Proceedings of the 1st International MobiSys Workshop on Mobile Opportunistic Networking*, pp. 62–66, New York, NY, USA, June 2007.

[25] A. Al-Hinai, H. Zhang, Y. Chen, and Y. Li, "Tb-snw: trust-based spray-and-wait routing for delay-tolerant networks," *The Journal of Supercomputing*, vol. 69, no. 2, pp. 593–609, 2014.

[26] M. Y. Mir and C.-L. Hu, "Exploiting mobile contact patterns for message forwarding in mobile opportunistic networks," in *Proceedings of the 2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, Seoul, Korea (South), May 2020.

[27] C. Wang, D. Wang, Y. Tu, G. Xu, and H. Wang, "Understanding node capture attacks in user authentication schemes for wireless sensor networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, p. 1, 2020.

[28] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceedings of the 2005 ACM*

SIGCOMM Workshop on Delay-Tolerant Networking, pp. 252–259, New York, NY, USA, August 2005.

[29] S. Shabalala, Z. Shibeshi, and K. Khalid, "Design of energy-aware prophet and spray-and-wait routing protocols for opportunistic networks," in *Proceedings of the International Conference on Wireless Intelligent and Distributed Environment for Communication*, pp. 35–46, Manhattan, NY, USA, 2018.

[30] N. Gupta, J. Singh, S. K. Dhurandher, and Z. Han, "Contract theory based incentive design mechanism for opportunistic IoT networks," *IEEE Internet of Things Journal*, p. 1, 2021.

[31] L. Yao, Y. Man, Z. Huang, J. Deng, and X. Wang, "Secure routing based on social similarity in opportunistic networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 594–605, 2015.

[32] F. Li and Y. Si, "Trust-based security routing decision method for opportunistic networks," *Journal of Software*, vol. 29, no. 9, pp. 2829–2843, 2018.

[33] M. Yao and S. Zhang, "Energy balanced routing algorithm based on community in opportunistic networks," *Journal of Chinese Computer Systems*, vol. 39, no. 9, p. 5, 2018.

[34] Z. Duan and Y. Yang, "Opportunistic forwarding algorithm based on connection time in probabilistic routing," *Microelectronics & Computer*, vol. 35, no. 12, pp. 50–54, 2018.

[35] J. Yuan, Z. Zhang, and W. Yang, "Data forwarding scheme based on social trust in opportunistic networks," *Computer Engineering and Design*, vol. 36, no. 8, pp. 2011–2015, 2015.

[36] M. Liu, Z. Chen, and J. Wu, "Design and implementation of routing security in mobile opportunistic networks," *Electronic Technology & Software Engineering*, vol. 134, no. 12, Article ID 244, 2018.

[37] X. Yang, T. Liang, and X. He, "Opportunistic routing based on node connectivity for wireless sensor networks," *Journal of Chinese Computer Systems*, vol. 40, no. 11, p. 24, 2019.

[38] Q. F. Zhang, C. Gui, Y. Song, B. L. Sun, and Z. F. Dai, "Routing algorithm in opportunistic networks based on node mobility," *Journal of Software*, vol. 32, no. 8, pp. 2597–2612, 2021, in Chinese.

[39] Q. W. Wang, Q. Qi, W. Cheng, and D. Li, "Node degree estimation and static game forwarding strategy based routing protocol for ad hoc networks," *Journal of Software*, vol. 31, no. 6, pp. 1802–1816, 2020, in Chinese.

[40] P. Kumar, N. Chauhan, and N. Chand, "Node activity based routing in opportunistic networks," in *Proceedings of the International Conference on Futuristic Trends in Network and Communication Technologies*, pp. 265–277, Manhattan, NY, USA, 2018.

[41] A. Vahdat and D. Becker, "Epidemic routing for partially-connected ad hoc networks," *Handbook of Systemic Autoimmune Diseases*, 2000.

[42] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," in *Proceedings of the International Workshop on Service Assurance with Partial and Intermittent Resources*, Berlin, Heidelberg, 2004.

[43] J. Chen, G. Xu, X. Wu, F. Wei, and L. He, "Energy balance and cache optimization routing algorithm based on communication willingness," in *Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–6, Nanjing, China, March 2021.

[44] Y. Yun-hui, X. M. Wang, L.-C. Zhang, S. Liu, and Y.-G. Lin, "An encounter-based routing algorithm for social opportunistic networks," *Computer Technology and Development*, vol. 028, no. 002, pp. 64–68, 2018.

[45] Z. Wang, X. Wang, and J. Sui, "Extending research for one simulator of opportunistic network," *Application Research of Computers*, vol. 29, no. 1, 2012.