Node Incentive Mechanism in Selfish Opportunistic Network

Hao-tian WANG[1,2], Zhi-gang Chen[1,2,*], Jia WU[1,2,*], Lei-lei WANG[1,2]
[1] School of Software, Central South University
Changsha 410075, China
[2] "Mobile Health" Ministry of Education-China Mobile Joint Laboratory
Changsha 410083, China
[e-mail: czg@csu.edu.cn;jiawu5110@163.com]
*Corresponding author: Zhi-gang Chen;Jia Wu

Received June 29, 2018; revised September 6, 2018; accepted September 30, 2018; published March 31 2019

Abstract

In opportunistic network, the behavior of a node is autonomous and has social attributes such as selfishness.If a node wants to forward information to another node, it is bound to be limited by the node's own resources such as cache, power, and energy.Therefore, in the process of communication, some nodes do not help to forward information of other nodes because of their selfish behavior. This will lead to the inability to complete cooperation, greatly reduce the success rate of message transmission, increase network delay, and affect the overall network performance. This article proposes a hybrid incentive mechanism (Mim) based on the Reputation mechanism and the Credit mechanism.The selfishness model, energy model (The energy in the article exists in the form of electricity) and transaction model constitute our Mim mechanism. The Mim classifies the selfishness of nodes and constantly pay attention to changes in node energy, and manage the wealth of both sides of the node by introducing the Central Money Management Center. By calculating the selfishness of the node, the currency trading model is used to differentiate pricing of the node's services. Simulation results show that by using the Mim, the information delivery rate in the network and the fairness of node transactions are improved. At the same time, it also greatly increases the average life of the network.

Keywords: Selfish node; Incentives; Cooperative; Diversity; Hybrid Mechanism (Mim); Credit; Reputation;

1. Introduction

Opportunistic network is an ad hoc network that does not require a complete link between the source node and the target node, and uses the node mobility [1] to meet with other nodes to realize communication.In the field of opportunistic network communications, researchers currently focus on how to ensure the feasibility of the network and the integrity of the data, and there are relatively few documents on how to increase the degree of cooperation of the nodes.The communication of the Opportunistic network node is based on the node's movement and cooperation. Once the node does not participate in the cooperation, it will inevitably affect the performance of the network and reduce the network delivery rate.In general, due to resource limitations, some nodes may not forward data packets of other nodes. In the study of opportunistic networks, this kind of behavior is called selfish behavior.In many cases, selfish behavior is also called a Drop attack [2-5].

Unlike the rational nodes in traditional routing protocols, in actual applications, nodes may be subject to pressure from many aspects, and nodes tend to exhibit selfishness [7].The behavior of a node usually has a certain sociability [8], such as the node is only willing to help a group forward the message.This node that refuses to forward messages for other nodes is called a selfish node [9].The selfish behavior of a node can also be understood as a cooperation problem between nodes.At present, the research work on the selfish behavior of nodes is mainly concentrated in the following three directions.

- How to effectively monitor the selfish behavior of nodes and divide these selfish nodes from the network.
- Exploring the impact of node selfish behavior on network performance
- Design effective strategies to motivate selfish nodes to participate in messaging in the network

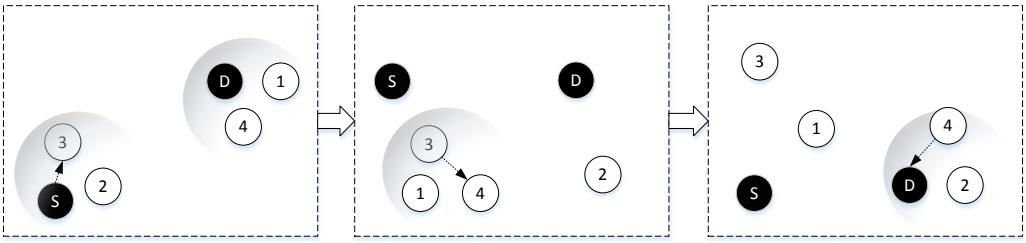

Fig. 1. Opportunistic Network Communication Diagram

Traditional ad hoc network usually rely on infrastructure, and all research on this network is based on the assumption that there are definite end-to-end links. However, opportunistic networks usually do not depend on infrastructure, and there may not be end-to-end connectivity throughout, which requires relying on the movement of nodes and the opportunities brought by encounters for data forwarding.For example, **Fig. 1** is a schematic diagram of an opportunistic network node communication. The S node is the source node and wants to forward the data to the target node D. However, S is not a direct neighbor of D. It is bound to encapsulate the data into a message and send it to the neighbor node 3 Or 2.We can see that in the figure, node 3 accepts the message of the source node S, and sends the message

to node 4 through the movement, and the final node 4 passes the message to the destination node D, thus completing the entire route communication.However, because the node is limited by its own resources, it usually has social attributes such as selfishness.If node 2 and node 3 show the selfishness of the node in the process of transmitting information, then the message arriving at the destination node from the source node will not be transmitted easily, thereby increasing the network delay and reducing the performance of the network.

There are three main causes [10] of selfish behavior. The first is because of resource problems in the network. Nodes assist in forwarding data packets while also occupying their own cache space and consuming their own energy. When data packet forwarding is performed as a relay node, the node can easily generate selfish behavior without any benefit.The second is the security problem in the network, because the node helps to forward the message may lead to leakage of their own information, which greatly increases the probability of their own attacks [11] by malicious nodes, thereby hurting their own interests.The third kind is that in some currency-based incentive strategies, virtual currency is used as a reward node to participate in data packet forwarding rewards. Nodes can use virtual currencies to buy content they are interested in and content forwarding services. This leads to deliberate deception and counterfeiting of certain nodes to obtain more virtual currency. The illusion that he successfully participated in the data packet forwarding, but in fact did not participate in forwarding.

According to the behavior of the node, the selfish behavior of the node can be divided into Drop and Non-Forwarding [12].The former is a node that participates in route forwarding and accepts messages from other nodes, but does not forward and discard these messages directly.The latter means that the node does not participate in route forwarding and directly refuses to receive messages delivered by other nodes.

Previous experiments show that when the number of selfish nodes increases by 10%-40%, the network delivery rate decreases by 16%-32% [13].When there are malicious nodes[14] in the network, the delivery rate of the network is lower.

Aiming at selfish and malicious nodes in opportunistic networks, this paper proposes a Mim mechanism based on Reputation mechanism[15] and Credit mechanism [16] that aims to reduce the impact of selfish nodes in an opportunistic network.In the Mim mechanism, there are three modules: selfishness, energy and transaction.The selfishness of the node is obtained through partial selfishness(the selfishness of a node to its cooperating nodes) and full selfishness(In addition to the selfishness of its cooperating nodes).In the energy module, we introduce a history record matrix [17] to record the energy of the node and the size of the forwarded message.In order to suppress the selfishness of nodes, we introduce virtual currency [18] to reward those nodes that successfully cooperate.We can always know the remaining energy of the node. When forwarding messages, the source node will preferentially select those nodes with high energy as relay nodes.Because energy also acts as a factor affecting the relay node's trading quotes.In the transaction module, the candidate relay node will give the source node a quote through its own attributes (selfishness, energy, etc.).The source node selects the optimal relay node based on the service quotation.Because there will be malicious nodes with false quotes, we have introduced the Central Money Management Center. This will make the node's wealth status transparent.When the transaction is successful, the source node will pay a certain fee according to its selfishness.Similarly, the relay node will also receive a certain monetary reward according to its selfishness.We chose Credit and Reputation strategies to compare our proposed Mim mechanism because it has proven to have good results compared to the previous existing mechanisms.

- As the proportion of selfish nodes in the network increases, the Mim mechanism has significant advantages over the Reputation policy and the Credit mechanism in terms of message delivery rate, average energy consumption, and average delay.
- By contrast, the central currency management center introduced in the Mim mechanism makes the wealth of both parties in a transparent state. Therefore，it can greatly eliminate the influence of false quotes from malicious nodes in the network.
- Because the energy of the nodes in the Mim mechanism is always concerned, those nodes with more available energy will have a higher probability of being able to forward messages.Experiments show that the energy mechanism in the Mim mechanism can effectively improve the average life of the node.

The following section presents notions about altruism model-ing in practice and describes other similar solutions in opportunistic networks, as well as several incentive mechanisms.Section 3 describes in detail the system model of the Mim mechanism.Section 4 compares the results of Mim and the other two mechanisms in three different scenarios,while Section 5 presents conclusions and future work.

2. Related Work

2.1 Three incentive mechanisms

From the existing research results of self-interest opportunity network incentives, designing and deploying incentives is considered to be the key to solving selfish problems.This section introduces the concept of altruistic modeling in practice and describes the incentive mechanisms for similar solutions to be used in opportunistic networks.By introducing the game theory in economics, modeling the nodes in the opportunistic network and designing the incentive mechanism of the nodes are the main methods to suppress the selfishness of the nodes.At present, there are mainly three incentive strategies to solve the problem of selfishness of nodes, that is, TFT-based(Tit-for-Tat) [19], Reputation-based, and credit-based.The TFT-based strategy is considered to be the simplest strategy to solve the selfish behavior of nodes.The strategy based on the Reputation is to reward and punish the reputation value maintained by the node, thus facilitating the cooperation of the selfish nodes.Based on credit, virtual credit is used as a node to forward the reward of data packets to stimulate the enthusiasm of selfish node cooperation.

Although, several strategies mentioned above have important reference significance for the design of the opportunistic network incentive mechanism.However, the blind pursuit of motivating node cooperation does not consider the impact of the node's own state on the entire network communication life, it may also lead to a lower message delivery rate in the network.For example, when the energy [20] of the node itself is insufficient, if only the cooperation between the nodes is pursued, the node can only die due to premature exhaustion of energy under the stimulation of the incentive mechanism.

2.1.1TFT mechanism

TFT mechanism is a symmetrical reciprocal mechanism, and it is also a trading-based incentive mechanism.This mechanism does not require the establishment of a reputation center. It is completed through fair trade between nodes and is characterized by easy implementation and scalability.TFT (Tit-for-Tat) incentive mechanism applied to delay tolerant network.The TFT mechanism guarantees the fairness of node transactions, and the

node selects interested messages to perform transactions according to itself, which enhances the enthusiasm of nodes to participate in message forwarding.The main idea of the TFT-based mechanism is to model the nodes based on the principle of symmetry reciprocity by introducing game theory.In the process of communication, one node helps another node to forward messages in the same amount of information. The TFT pairing scheme and the mutual exchange of messages are two major schemes for implementing this mechanism.

Shevade et al[21]. proposed a TFT-based routing algorithm IAR, which is also the first TFT-based node excitation mechanism in DTNs.In this algorithm, Chebyshev inequality is used to estimate message delivery rate and the exponential weighted moving average method(EWMA:exponentially weighted moving average) is used to predict future business demand. The message delivery rate is then optimized under the constraint that the nodes forward the same amount of data to each other.The self-private node determines whether the previous time unit has forwarded enough data for other nodes. If the amount of data is greater than the amount of data to be sent in the next time unit, then this node will not provide additional data services for other nodes.The IAR also adopts a repentance mechanism. When a node judges the behavior of other nodes, it not only refers to the data that other nodes forward this time, but also refers to the amount of data that it has forwarded for the other node.Zhou H et al[22]. proposed a Consub based on TFT strategy. The scheme evaluates the forwarded data. The incentive node participates in the forwarding of data in exchange for the data they are interested in. Each node maintains a list to record the data of interest and the lifetime of the data.When the nodes meet, the two nodes exchange list information with each other. The data is then evaluated. Taking into account the two factors of the possibility of meeting and the cooperation level between nodes, the exponential distribution is used to describe the possibility of meeting between nodes. The cooperation level is calculated according to the average number of data exchanged for each node encounter.Prioritize content value by prioritizing caching and distributing high-value data. When the cache space is insufficient, the high-value data will replace the low-value data in the cache, thus obtaining the maximum benefit.

Because the constraints are too many.TFT mechanism encourages selfish node cooperation to have some limitations.First, one of the two nodes that meets the node stores little information, that is, when the service in the network is severely asymmetric, the mechanism will cause network performance degradation. For example, node A carries the message that the destination node is B, If there is no message in the cache of Node B,then node A will not forward any message, so the efficiency of the message in the network is greatly reduced.

2.1.2 Reputation mechanism

Reputation-based incentive mechanism mainly have two methods: one is a penalty mechanism, when the node is determined to be a selfish node, punitive measures are taken to achieve the effect of incentive; the other is an incentive measure, which is different for nodes with different reputation values. The treatment approach to achieve the incentive effect.The main idea of the mechanism based on the Reputation is that the node needs to maintain and update a table for recording the reputation of other nodes.In the process of transmitting messages, the source node judges whether it can be trusted through the behavior of other nodes, and usually selects those nodes with higher reputation to help them forward the messages.Vinicius F.S d the MINEIRO mechanism, put forward according to the different reputation value different income method, through the limit conditions for Bayesian [23] game algorithm, promote network to reach a Bayesian Nash equilibrium [24].

Bigwood G et al[25]. proposed an IRPNMAN mechanism. In the network, the node maintains a table of record reputation.This table will be updated when two nodes meet.Use this table to judge the degree of cooperation of nodes in the network.The specific algorithm is as follows: Assume that node A has a message to transmit node C, but node A first encounters node B, and hopes that node B acts as a relay node.But Node B is defined as a selfish node in the network, then other nodes will not forward B as a message sent by the source node.Node B can only obtain the reputation value by means of acting as a relay node.Until Node B's reputation value is greater than the threshold set in the network, Node B can get rid of the label of the selfish node.Through the penalty mechanism of the strategy, the self-private nodes in the network are encouraged to participate in data forwarding.

The MINEIRO strategy proposed by Vinicius F.Sd et al. brings the network to a Bayesian equilibrium through Bayesian games.This strategy mainly uses different revenue methods based on the reputation value of the node.Dividing nodes into altruistic nodes, rational nodes, and selfish nodes.The specific algorithm is as follows: Only when the node acts as a relay node to forward messages of other nodes can increase the revenue, otherwise the revenue decreases.The reputation value of the rational node ranges between 0 and 1, which means that the rational node is mainly inclined to balance its own reputation value.Calculate the income based on the performance type of the node.Through experimental comparison, there will be a range, so that the reputation value of the node will get the maximum benefit under this range, and then the Bayesian equilibrium that each node is willing to participate in message forwarding is achieved.

However, the reputation mechanism will also have some restrictions in stimulating the participation of selfish nodes.The node cannot separate the nodes above the threshold. It will think that as long as the nodes above the threshold have the same reputation, the incentive effect achieved is not ideal.

2.1.3 Credit mechanism

The main idea of a mechanism based on Credit is that a node earns credit by forwarding messages to other nodes.By introducing the concept of virtual currency, the mechanism compares the message forwarding process to a transaction process.If the destination node of the message pays gratuity for the delivered message, then this scheme is a message transaction scheme. If the source node pays for the delivery of the message, then this scheme is a message gratuity scheme.

Yun Li et al. proposed a monetary incentive mechanism BIP [26]. In this policy, using the node bargaining model, the node is allowed to pay and charge based on its status and message attributes.Each node maintains its own data list, containing the residual cache space, the wealth it has, and the lifetime of the information. And defines the distribution of data packet is the buyer, buy forward service for node, receiving data grouping of relay nodes are the seller, the purpose is to sell forward data packet to earn virtual currency.The specific algorithm is as follows: When node a and node b meet, node a is the request node, and bid M is sent to node b to purchase the forwarding service.The lower the message's message living space and remaining cache, the lower the price M.At the same time, M is also affected by the amount of wealth and information size of node a.Node b as a relay node will also submit a service offer m to node a as a reward for forwarding messages by itself.The size of m is proportional to the message size and the wealth of node b, and inversely proportional to the remaining buffer and consumed energy of node b.If the node A gives M greater than the m proposed by the node b, then the transaction is successful, and the node a provides a certain wealth value as the seller's reward. Otherwise, the transaction fails.

For the Credit mechanism, as long as the node touches the forwarding mechanism, it is considered a successful transaction [25].Moreover, there will be no differential pricing of this transaction and other transactions, which will greatly lose the fairness.

3. Incentive Design

3.1 Selfishness of node

Based on the virtual currency and reputation values in Credit and Reputation strategies, this paper adopts a hybrid mechanism that calculates the selfishness of nodes through the historical behavior of nodes.Rewards those who successfully cooperate through virtual currency.In other words, the smaller the selfishness of the node, the more rewards the node receives after the transaction is completed.Here, we use the selfishness of the node as a pricing factor for the transaction price.

3.1.1 History matrix

Assuming that the number of nodes in a network is N, we can define a historical behavior record matrix within each node. When node *i* and node *j* have information transaction behavior in the network. Node *i* records the transaction behavior between them as (A_{ij}, T_{ij}).Here, we define A_{ij} as the number of messages that node j successfully forwards to node *i*.We define T_{ij} as the number of message forwarding requests received by node *j* from node i.In the initial state of the network, both A_{ij} and T_{ij} are 0. $A_{ij}=0$ represents that the number of messages received by node *j* from node *i* is 0, and $T_{ij}=0$ indicates that the number of messages forwarded by node *j* to help node *i* is 0.

If two nodes meet and a message needs to be forwarded, node *i* updates the matrix after forwarding the message. Node *j* agrees to help node *i* forward the message, then $A_{ij}=A_{ij}+1$, $T_{ij}=T_{ij}+1$. Node *j* refuses to help node *i* forward the message, $A_{ij}=A_{ij}+1$.Matrix completes the update.

3.1.2 Node selfishness

In the opportunistic network, the amount of messages forwarded by the node is limited.Because the node will provide message forwarding service to other nodes, it will consume its own resources.In the opportunity network, the resource of the node is relatively scarce, so when helping other nodes to forward the message, the node first judges its ability to forward the message through the message forwarding request sent by other nodes.In this article, we set a threshold ζ_b for nodes in the network.For example, if node *i* sends a message delivery request to node *j*, then node *j* first determines whether the amount of data to be forwarded is in $0 \le B_i \le \zeta_b$ .If the amount of messages sent by node i exceeds this threshold, the node will directly reject the request.It is not that node *j* does not want to help node *i* forward this data, but node *j* does not have the ability to forward this message.Usually this threshold ζ_b is 80% of the amount of information that the node can transmit.

Because the size of the message exceeds the defined threshold, it is a special case that the node has no ability to help other forwarded messages.For this case, it will not be substituted as a factor into the formula below we calculate the selfishness of the node. Therefore, this situation does not affect the selfishness of the service node to the served node.

Because nodes have certain social attributes, some nodes are only one or more selfless, so we distinguish the selfishness of nodes.Here we divide the selfishness of the node into partial selfishness and full selfishness.The partial selfishness of node *j* to node *i* is defined as: the probability that node *j* does not help node *i* forward the service， where $0 \le O_{ij}^{p} \le 1$. O_{ij}^{p} calculation formula is as follows：

$$O_{ij}^{p} = \frac{T_{ij} - A_{ij}}{T_{ij}} \tag{1}$$

Here we can see the evaluation formula of the partial selfishness of the node, and can more clearly understand the difference between the number of messages forwarded by A_{ij} as node *j* to node *i* and the total number of T_{ij} requests sent by node *i* to node *j*.We first calculate the partial selfishness of node *i*, we can see that its value ranges from 0 to 1.According to the values of A and B, the partial selfishness of nodes is divided into four cases:

- When A_{ij}=T_{ij}, that is to say node *j* accepts and forwards the all messages delivered by node *i*. At this point, the partial selfishness O_{ij}^{p} of node *j* to node i is 0.
- When A_{ij} = 0, then the node *j* has a selfishness of 1 for node *i*.In other words, node *j* did not succeed in helping node *i* forward the message once.
- When A_{ij} and T_{ij} are equal to 0 at the same time, it means that node *i* and node *j* do not meet, or there is no communication between the two nodes. At this time, node *j* does not exist for the partial selfishness O_{ij}^{p} of node *i*.
- When $A_{ij} < T_{ij}$, it indicates that message interaction is performed between node *j* and node *i*, and node *j* helps node *i* forward the message. At this time, the partial selfishness O_{ij}^{p} of node *j* to node *i* is $0 \le O_{ij}^{p} \le 1$.

Because according to the discrete random variable S, we get the sample $S_1, S_2 \cdots S_n$.When any node excluding node *i* sends a message delivery request to node *j*, if node *j* does not help forward message T takes 0. If node *j* helps forward message T takes 1.Therefore, the sample S conforms to the Bernoulli distribution. We can use Maximum Likelihood Estimate to find the full selfishness of node *i*.The formula for solving O_{ij}^{f} is as follows:

$$O_{ij}^{f} = \frac{\sum_{k=1,k\neq j}^{n} (T_{ij} - A_{ij})}{\sum_{k=1,k\neq j}^{n} A_{ij} + \sum_{k=1,k\neq j}^{n} (T_{ij} - A_{ij})} \tag{2}$$

The full selfishness O_{ij}^{f} of node *i* for node *j* is defined as the probability that node *i* does not forward messages for nodes other than node *j*, where $0 \le O_{ij}^{f} \le 1$.The full selfishness of a node is roughly divided into three cases according to the node communication in the opportunistic network.

- When the value of node *j* to node *i* full selfishness O_{ij}^{f} is equal to 1, it indicates that node *i* is excluded from the network, and node *j* has not forwarded any messages to other nodes.

- When the full selfishness O_{ij}^{f} of node *j* to node *i* is 0, it means that node *i* is excluded in the network, and node *j* forwards the message sent by other nodes.Of course, this situation is rare in the network.
- When the full selfishness O_{ij}^{f} of node *j* to node *i* is $0< O_{ij}^{f} <1$,it indicated that node *j* did not forward all messages transmitted by nodes other than node *i*

Therefore, the selfishness O_{ij} of node *j* to node *i*:

$$O_{ij} = \lambda O_{ij}^{p} + \omega O_{ij}^{f} = \lambda \frac{T_{ij} - A_{ij}}{T_{ij}} + \omega \frac{\sum_{k=1,k\neq j}^{n} (T_{ij} - A_{ij})}{\sum_{i=1,k\neq j}^{n} A_{ij} + \sum_{k=1,k\neq j}^{n} (T_{ij} - A_{ij})} \tag{3}$$

In equation (3), λ and ω represent the weight of selfish and total selfishness of node *j* to node *i*. According to experience, the values of λ and ω are both 0.5.

3.2 The energy mechanism of the node

3.2.1 The energy mechanism of the node

In this article, always pay attention to the changes of the node's own energy.In an opportunistic network, each node participating in this message will consume a certain amount of energy.With the consumption of the node itself, the energy of the node will continue to decrease with the flow of time.Due to the limited energy of the nodes, in order to ensure the connectivity rate in the opportunistic network, when searching for the relay nodes, the nodes find the energy-rich nodes to forward the messages as much as possible.Therefore, it can effectively prevent the node from generating selfish behavior due to lack of energy to extend the life span.

3.2.2 Historical data matrix for recording data size

As with message forwarding, there is a matrix within the node that records the amount of energy left by the node and the size of the total forwarded data.The matrix of node *i* about the remaining energy of itself and the size of the total amount of data forwarded before can be expressed as $(E_{i}^{r(t)}, B_{i}^{s(t)})$.

Where $E_{i}^{r(t)}$ represents the remaining energy of node *i* at time t, and $B_{i}^{s(t)}$ represents the total amount of data forwarded by node *i* before time *t*.In the opportunistic network, the initial node energy *E* is the same.Therefore, the formula for the remaining energy of node *i* at time t is as follows:

$$E_{i}^{r(t)} = E - (E_{i}^{c(t')} + E_{i}^{s(t')}) \tag{4}$$

We define $E_{i}^{c(t')}$ as the total energy consumed by node *i* for forwarding messages to other nodes prior to t time.The formula for the derivative of $E_{i}^{c(t')}$ is as follows:

$$E_{i}^{c(t')} = p * t'' \tag{5}$$

p represents the work and power consumed by the node when forwarding messages.In the opportunistic network, the specifications of the nodes are the same, so p is the same.We define t'' as the

cumulative time consumed by node *i* to forward messages for other nodes.

$$t'' = \frac{B_i^{s(t)}}{v} \tag{6}$$

In the previous article, $B_i^{s(t)}$ is defined as the size of the total amount of data that node *i* can help other nodes forward before t time.

$$B_i^{s(t)} = \sum_{e=1}^{n} B_i^e \tag{7}$$

The size of the data for each message forwarded by node *i* is defined as B_i^e . The result obtained by formula (7) is brought into formula (6) to obtain t''.By analogy, according to the obtained t'' into Equation (5), the total energy consumed by node *i* before forwarding time can be obtained.

Since the node has energy consumption at the time of not forwarding the message, here we use $E_i^{s(t')}$ to represent the energy consumed when node *i* is still before t.

$$E_i^{s(t')} = p' t''' \tag{8}$$

Where p' is the power at which the node is stationary and is a fixed value. t''' represents the time when the node was stationary before time t.

$$t''' = T_i - \sum_{e=1}^{n} t_i^e \tag{9}$$

T_i represents the time interval experienced by node *i* from start to t, and the time interval when the node *i* is still can be obtained by calculating the time $\sum_{e=1}^{n} t_i^e$ accumulated by the node *i* forwarding the message.

By bringing t''' into equation (7), we can find the energy consumed when node *i* is still before time t.Then, according to equations (8) and (5), the residual energy $E_i^{r(t)}$ of node *i* in equation (4) at time t can be obtained.

We set a threshold E_v for the energy of the node. When the energy of the node is lower than the threshold, the node will no longer help other nodes forward the message.In addition, considering that energy is gradually consumed during message forwarding.Node *j* needs node *i* to forward the message. If $E_i^{r(t)} - E_i^c \le E_v$, then node *i* will not forward the message.Based on experience, we set the value of E_v to 5 percent of the initial energy E .

3.3 Trading model

In a selfish opportunistic network, message forwarding can be abstracted as a transaction process.To this end, we introduced the concept of virtual currency.Virtual currency is used to motivate nodes to cooperate with each other, and the virtual currency is a fixed value in the mechanism based on Credit.

3.3.1 Central Money Management Center

To make nodes pay each other, we assume that there is a currency clearing center in the system.From another point of view, the introduction of the Central Money Management Center[27] can effectively prevent false quotes.Each node has its own account in this currency clearing center.Each transaction at each node is completed by the clearing house.The central money management center is connected to the Internet server, and as long as the node is connected to the Internet, the node can access the fee clearing center through the network.

When two nodes are traded, they can access the central money management center to learn about the other node's wealth.This can effectively avoid the issue of false quotes.When two nodes finish a transaction, both nodes will get a signed receipt and submit the receipt to the management center.The management center will clear the receipt after it is confirmed by the receipt. If the liquidation is successful, the management center will automatically charge a certain fee from the account of the node that receives the service.

3.3.2 Trading Rules

When nodes *i* and *j* enter each other's radio frequency range, if node *i* has a message that requires node *j* to facilitate forwarding, and node *j* agrees to forward. Then the two nodes start trading messages.According to the selfishness of node *i* and node *j* and the message's own attribute, node *j* gives a price M for this service.

$$M = B\{\mu(1-O_{ij}) + \beta(1-\frac{C(t)}{C}) + \xi(1-\frac{E_{j(t)}^{r}}{E}) + \psi(1-\frac{ul}{TTL})\} \tag{10}$$

Where B represents the size of the message, and O_{ij} is the selfishness of node *i* to node *j*.We define $C(t)$ as the cache space size for the current moment, and C represents the cache space size at the initial time. $E_{j(t)}^{r}$ is the current energy of node *j*, and E is the initial energy. ul indicates the remaining lifetime of the message and *TTL* indicates the initial lifetime of the message. μ, β, ξ and ψ are weight factors that indicate the degree of self-consistency, cache size, energy, and remaining message lifetime affect the message price.We define $\mu+\beta+\xi+\psi=1$. According to experience μ, β, ξ, ψ values are 0.45, 0.25, 0.05, 0.25 respectively.

If node *i* agrees with the price given by node *j*, then the transaction proceeds.At this point, both nodes will know the funds of the two sides through the Central Money Management Center.Preventing false quotes from nodes through the Central Money Management Center.When two nodes complete a transaction, both nodes will receive a signed receipt and submit the receipt to the Central Money Management Center. The management center will clear the receipt after confirming it is correct. If the liquidation is successful, the clearing house will automatically charge a certain fee in the node *i*'s account.

$$T = M(1-O_{ij})\eta \tag{11}$$

Where T represents the transaction tax charged by the Central Currency Management Center on this transaction.From the formula (11), the smaller the selfishness of the node *i*, the lower the tax paid after the transaction is completed. η is the weight of selfishness. Here we set its value to 0.05.

In order to reward the nodes involved in the cooperation, the Central Money Management Center will extract a part of the transaction tax of the node that received the service to reward the node that provides the service.

$$P = T(1 - O_{ji})\sigma \tag{12}$$

Where P represents the reward for node *j* providing services after the transaction.It can be seen that the lower the selfish reading of node *j*, the higher the reward obtained after the transaction is completed. σ is the selfishness weight of node *j*.Here we set its value to be 0.7.

Algorithm： Message forwarding

： Source node *i*, Relay node *j*
： Initialize the parameters of the node
1: Node *j* enters the RF range of *i*
2: Node *i* sends a message delivery request to node *j*
3:The node j determines whether the amount of messages forwarded by the help node i exceeds ζ_b.
4:if the message size does not exceed the threshold then
5:Node *j* considers whether to agree to the messaging request
6: **if** Node *j* agrees to help node *i* forward messages **then**
7: Calculate the selfishness O_{ij} and O_{ji} of node *i* and node *j*
8: Calculate the current residual energy of node *j*
9: **if** $E_{j(t)}^{r} > E_v$ **then**
10: *j* calculate the quote M
11： *j* sends a quote M to *i*
12: **if** *i* agrees with *j*'s quote **then**
13: *i* checks the wealth status of *j* of the Central Money Management Center through the network
14： **if** *j*'s wealth meets quotation M **then**
15： *i* passes message and check to *j*
16： Node *j* sends receipt and check to the Central Money Management Center
17： Calculate transaction fee T
18： Calculate reward P
19： The Central Money Management Center collects fees from *i*'s account and adds bonus to *j*'s account
20： Transaction complete
21： $A_{ij}=A_{ij}+1$
22： $T_{ij}=T_{ij}+1$
23： **end if**
24： **end if**
22: **end if**
25： **else** $A_{ij}=A_{ij}+1$
26: **end if**
27:**end if**

4. Experimental Results and Analysis

4.1 Simulation settings

The Epidemic[28] algorithm was proposed by Amin Vahdat et al.In this routing algorithm, the

distribution of messages in the network is similar to the spread of infectious diseases.When a node carrying a message encounters a node that does not carry a message, a copy of the message is generated to deliver the message.The node that delivered the message stores the message in its own cache and continues to forward the message according to this operation. Until the message is delivered to the destination node or the message has a lifetime of zero.Amin Vahdat puts forward three goals in the article, which are divided into:

- Minimize resource consumption.
- Minimize data latency.
- Maximize data transmission success rate.

In the Epidemic algorithm, the buffer area of the node stores data packets forwarded by the source node and the relay node, and each data packet has a unique identifier.Each node needs to maintain a hash table to record which data packets are stored in the node cache. When two nodes meet, the two nodes exchange their own hash tables to learn the data packets that are not in the cache, and then pass them. The data group that the other party does not have.

This article uses ONE as a simulation platform.At the beginning of the simulation, the nodes are initialized and the EPIDEMIC routing algorithm is used as the background.Using the Reputation Strategy and the Credit Strategy as references, the message delivery rate, average delay, and average energy consumption are selected as performance parameters to verify the performance of the incentive mechanism.

Table 1. Simulation settings

Environmental parameter	Settings
Simulation time/h	15
Simulation area	10000 m×15000 m
Background city	St Paul
Number of nodes	150
Velocity of a node /(m·s^{-1})	0.5~1.5
Transmit speed/(KB·s^{-1})	250
Maximum transmission distance /m	10
Transmission mode	broadcast
Buffer size/MB	10
Packet size	500KB~1MB
Event interval/s	25~35
TTL/h	5
Initial energy/J	2500
Power when no message is forwarded/W	0.5
Transmission power/W	1
Proportion of malicious nodes	[0,0.2,0.4,0.6,0.8,1]
Proportion of selfish nodes	[0,0.2,0.4,0.6,0.8,1]
Maximum number of running rounds	2500

4.2. Performance parameters

This paper selects the message delivery rate, average delay and average energy consumption as performance parameters to verify the nature of the Mim policy.EMim, ERepputation, and ECredit indicate the addition of Mim mechanism, Reputation, and Credit mechanism based on the EPIDEMIC routing algorithm.

4.2.1 Message delivery rate

The message delivery rate DR refers to the ratio of the number M_{arrived} of messages arriving at the destination node in the opportunistic network to the total number of generated messages M_{created}.

$$DR=\frac{M_{\text{arrived}}}{M_{\text{created}}}\times 100\% \tag{13}$$

4.2.2. Average delay

Average delay AD refers to the average time it takes for a message to be delivered to be delivered successfully.

$$AD=\frac{\sum_{i=0}^{NUM_{\text{d}}}(T_{i\text{end}}-T_{\text{istart}})}{NUM_{\text{d}}} \tag{14}$$

Where $T_{i\text{end}}$ represents the time for the message to arrive at the destination node, T_{istart} represents the time generated by the message, and NUM_{d} represents the total number of messages that were successfully forwarded.

4.2.3. Average energy consumption

The average energy consumption EC refers to the average energy consumed by nodes in the network to forward messages.

$$EC=\frac{E_{\text{init}}-E_{\text{left}}}{NUM_{d}} \tag{15}$$

Where E_{init} represents the initial energy of the previous simulation node, E_{left} represents the residual energy of the node after the simulation is completed, and NUM_{d} represents the total number of successfully forwarded messages.

4.3. Simulation result analysis

4.3.1.The effectiveness of Mim mechanism

The proportion of selfish nodes is defined as the percentage of selfish nodes in the network.Figure 1 shows the delivery rate of EMim mechanism, EReputation policy and ECredit policy under different selfish ratios.

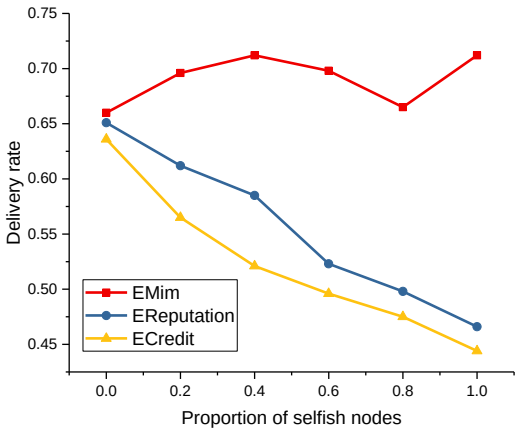

Fig. 2. Delivery rate under different selfishness ratio

According to **Fig. 2**, we can see that with the increase in the number of selfish nodes in the network, the delivery rate of the EReputation mechanism and the ECredit mechanism is getting lower and lower, while the EMim mechanism has been maintained at a relatively high level.This is because of the EReputation mechanism and the ECredit mechanism, and the selfish node refuses to forward messages to other nodes.With the EMim mechanism, virtual currency is used to reward participating nodes so that they can help other nodes to forward messages. Therefore, the message delivery rate has been maintained at a relatively high level.

In opportunistic network, not all nodes can participate in message forwarding, so it is very likely that the optimal path will be missed.Under the conditions of the three strategies, the average delay is shown in **Fig. 3**.

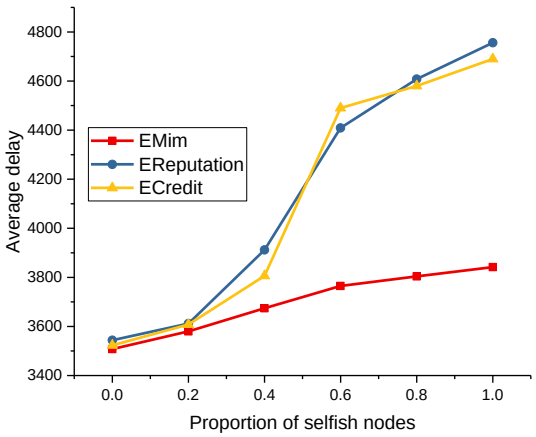

Fig. 3. Average delays under different selfish ratio

As can be seen from **Fig. 3**, when EReputation mechanism and ECredit mechanism are used, the average delay increases significantly as the proportion of selfish nodes increases.On the contrary, when using the EMim mechanism, the average delay has only small changes as the proportion of selfish nodes increases.This is because the adoption of the EMim mechanism greatly mobilizes the enthusiasm of the nodes to participate in cooperation by linking

selfishness with virtual currency.

Different from the EReputation mechanism and the ECredit mechanism, the EMim mechanism has a higher degree of motivation than the former. This also results in the nodes being more likely to participate in the cooperation. Compared with both, the average energy consumption of the EMim mechanism nodes is higher.

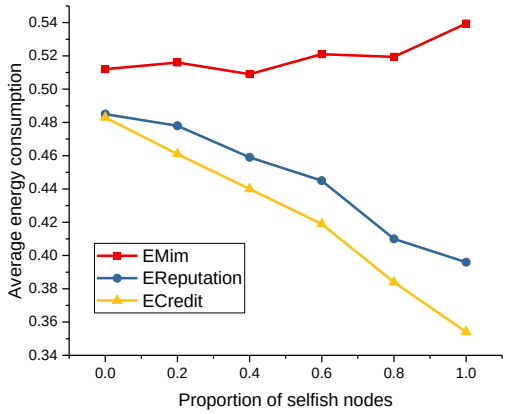

Fig. 4. Average energy consumption under different selfish ratio

From **Fig. 4**, it can be shown that the EMim mechanism is more effective than the EReputation mechanism and ECredit mechanism in motivating node cooperation.

4.3.2.Suppress performance of false quotes

In the EMim mechanism, the Central Currency Management center was introduced to make the node's account state relatively transparent, so to some extent, the node's false quotation was suppressed.We define the false quoted node as a malicious node. The proportion of malicious nodes is defined as the ratio of malicious nodes to the total number of nodes in the network.

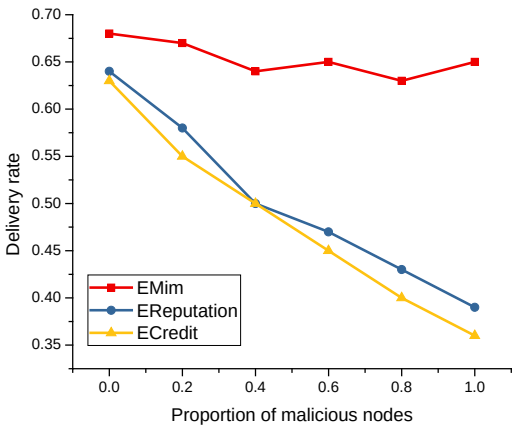

Fig. 5. Delivery rate under the proportion of different malicious nodes

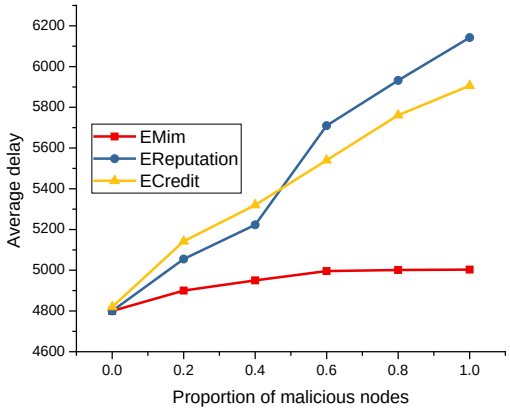

Fig. 6. Average rate under the proportion of different malicious nodes

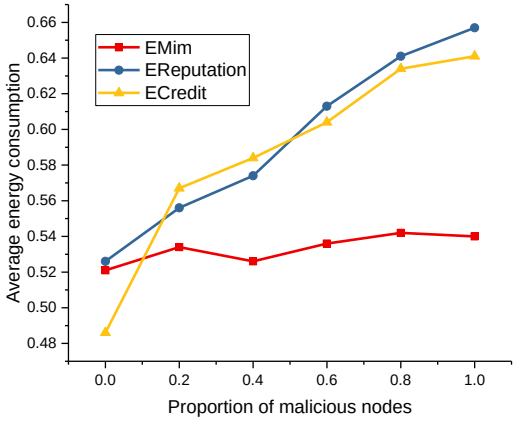

Fig. 7. Average energy consumption under the proportion of different malicious nodes

Because there is a mechanism for suppressing false quotation in the EMim mechanism, this paper compares the EMim mechanism with the EReputation mechanism and the ECredit mechanism. From **Fig. 5** to **Fig. 7**, it can be seen that the EMim mechanism can not only suppress false quotes, but also perform slightly better in terms of message delivery rate, average delay, and average energy consumption.This is because the node's account information is public in the EMim mechanism. The two sides can learn about each other's wealth status from the central money management center through the network, so that the behavior of the false quotes of the node is immediately dismantled.

4.3.3.The impact of energy and message cache space

The survival of a node requires energy to maintain, and it requires a lot more energy when the node forwards the message.Once the energy is exhausted, it means the death of the node.Dead nodes will not be able to participate in cooperation.In order to ensure the delivery rate of the network, the node's survival time should be extended as much as possible.

Fig. 8 shows the change in the number of node deaths as the number of rounds of network operations increases for the three strategies.It can be seen that the EReputation mechanism shows that the first death node is around 900 rounds, and 50 percent of death nodes are around 1200 rounds. All the nodes die around 1600 rounds. ECredit mechanism appears with the first death node at around 1,000 rounds, with 50 percent of the dead nodes being around 1300 rounds and all the nodes dying at about 1600 rounds.Relatively speaking, the first death node of the EMim mechanism was around 1200 rounds. Fifty percent of the node deaths occurred around 1600 rounds, and all the nodes died around 1800 rounds.It is clear that the Emim mechanism is better than the previous two strategies.In EMim mechanism, when a node forwards a message, it is preferred to select the nodes that are energetic through the quotation mechanism.In this way, those nodes with less remaining energy can be brought into a certain buffer space, thus improving the life cycle of the network and ensuring the stable and continuous progress of the network.

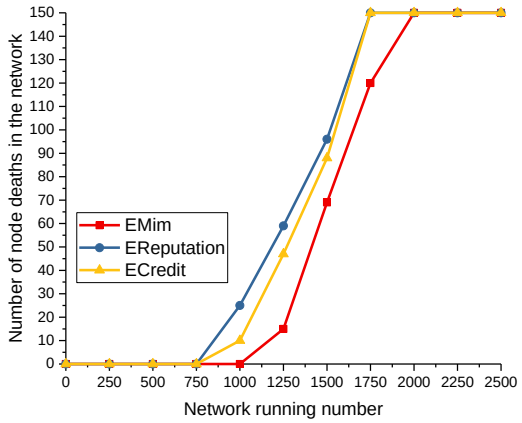

Fig. 8. Number of dead nodes in the network

There is a cache space for messages from generation. When the buffer space of the message is very low, it may cause the message to die and affect the delivery rate.Therefore, as the initial cache space of the message increases, the delivery rate of the message also increases.

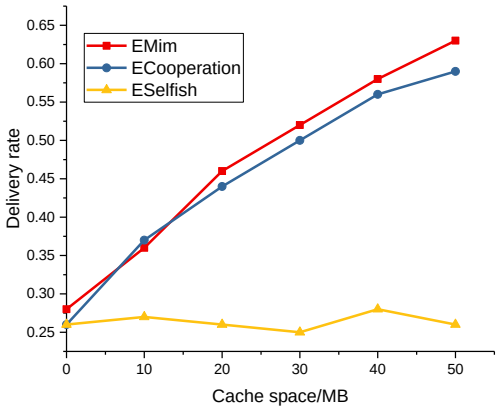

Fig. 9. Number of dead nodes in the network

In **Fig. 9**, ECooperation and ESelfish respectively represent the EPIDEMIC routing algorithm for all cooperative nodes and all selfish nodes in the network.Because ESelfish uses a direct delivery model, changes in cache space have little impact on delivery rates.For ECooperation mechanism and EMim mechanism, the delivery rate gradually increases as the cache space increases. Message overflow occurs when the node helps the other nodes to forward the message if the cache space is too small.

5. Conclusion

In this study, we propose a hybrid incentive mechanism based on self-property opportunistic network routing and forwarding mechanism.Positive Mim mechanism from both theoretical and experimental aspects can effectively motivate nodes to cooperate with each other.Through the introduction of the concept of the Central Money Management Center, the problem of false quotations between nodes and the high selfishness of the nodes due to their own social attributes have been solved.The energy mechanism proposed in the Mim mechanism can effectively extend the service life of the network, thereby reducing network delay and improving network throughput.

However, in the Mim mechanism, only the effects of node selfishness and energy on node behavior are considered. Actual influencing factors include node memory, node living environment.The incentive mechanism of this paper aims to motivate the selfish nodes to cooperate with each other and does not consider the packet loss behavior caused by the complexity of the nodes after the transaction is completed.The future should further consider the influence of many factors on the behavior of selfish nodes.

Acknowledgment

This work is supported by the National Natural Science Foundation of China (Grant No.71633006, Grant No. 616725407). This work is supported by the China Postdoctoral Science Foundation funded project (Grant No. 2017M612586). This work is supported by the Postdoctoral Science Foundation of Central South University (Grant No. 185684). Also, this work was supported partially by ”Mobile Health” Ministry of Education - China Mobile Joint Laboratory.

References

[1] Wu J, Chen Z G and Zhao M, “Effective information transmission based on socialization nodes in opportunistic networks,” *Computer networks*, Vol. 129, Part 1, 297-305, December 24, 2017. Article (CrossRef Link).

[2] Burgess J, Bissias G D, Corner M D, et al., “Surviving attacks on disruption-tolerant networks without authentication[C],” in *Proc. of ACM international symposium on Mobile ad hoc networking and computing*, 61-70, 2007. Article (CrossRef Link).

[3] Li F, Wu J, Srinivasan A, “Thwarting Blackhole Attacks in Disruption-Tolerant Networks using Encounter Tickets [C],” in *Proc. of IEEE INFOCOM 2009*, 2428-2436, 2009. Article (CrossRef Link).

[4] Lilien L, Kamal Z H, Bhuse V, et al., “The Concept of Opportunistic Networks and their Research Challenges in Privacy and Security [J],” *Mobile and Wireless Network Security and Privacy*, 85-117, 2007. Article (CrossRef Link).

[5] Lindgren A, Hui P, "The quest for a killer app for opportunistic and delay tolerant networks:(invited paper) [C]," in *Proc. of the 4th ACM workshop on Challenged networks*, 59-66, 2009. Article (CrossRef Link).
[6] Boldrini, Chiara, M. Conti, and A. Passarella, "Exploiting users' social relations to forward data in opportunistic networks: The HiBOp solution," *Pervasive and Mobile Computing*, Vol. 4, no. 5, 633-657, 2008. Article (CrossRef Link).
[7] Xiao M, Wu J, Huang L, "Community-Aware Opportunistic Routing in Mobile Social Networks[M]," *IEEE Transactions on Computers*, Vol. 63, no. 7, 1682-1695, 2014. Article (CrossRef Link).
[8] Wu J, Chen Z G, "Sensor communication area and node extend routing algorithm in opportunistic networks," *Peer-to-Peer Networking and Applications*, Vol. 11, no. 1, 90–100, January 2018. Article (CrossRef Link).
[9] Das D, Majumder K, Dasgupta A, "Selfish Node Detection and Low Cost Data Transmission in MANET using Game Theory [J]," *Procedia Computer Science*, Vol. 54, 92-101, 2015. Article (CrossRef Link).
[10] Wang, Eric Ke, et al., "Analyzing Selfish Behavior in Opportunistic Networks," in *Proc. of 2017 14th International Symposium on Pervasive Systems, Algorithms and Networks & 2017, International Conference on Frontier of Computer Science and Technology & 2017 Third International Symposium of Creative Computing (ISPAN-FCST-ISCC)*, 218-225, 2017. Article (CrossRef Link).
[11] M. Jo, L. Han, D. Kim and H. P. In, "Selfish attacks and detection in cognitive radio Ad-Hoc networks," *IEEE Network*, vol. 27, no. 3, 46-50, May-June 2013. Article (CrossRef Link).
[12] Li Y, Su G, Wang Z, "Evaluating the effects of node cooperation on DTN routing[J]," *AEU - International Journal of Electronics and Communications*, Vol. 66, no. 1, 62-67, 2012. Article (CrossRef Link).
[13] Xu N,Rangwala S, Chintalapudi K, et al., "AA wireless sensor network for structural monitoring [C]," *in Proc. of the ACM Conference on Embedded Networked Sensor Systems.Baltimore MD*, 2004.
[14] Alajeely M, Ahmad A, Doss R, "Malicious Node Traceback in Opportunistic Networks Using Merkle Trees[C]," in *Proc. of 2015 IEEE International Conference on Data Science and Data Intensive Systems*, 147-152, 2015. Article (CrossRef Link).
[15] Liu L, "A Survey on Reputation-Based Incentive Mechanism in Opportunistic Networks[J]," *Applied Mechanics and Materials*, Vol. 543-547, 4288-4290, 2014. Article (CrossRef Link).
[16] Liu H, Lee P P C, Lui J C S, "On the credit evolution of credit-based incentive protocols in wireless mesh networks[J]," *Computer Networks*, Vol. 57, no. 17, 3327-3343, 2013. Article (CrossRef Link).
[17] Hui-Juan L I, Zhang Z Y, Yang W Z, et al., "Node incentive mechanism in opportunistic networks[J]," *Computer Engineering and Design*, 2016. Article (CrossRef Link).
[18] Alese B K, Thompson A F, Oni P Y, "A location privacy system in mobile network using game theory[C]," in *Proc. of International Conference on Cyber Situational Awareness, Data Analytics and Assessment*, pp. 1-5, 2017. Article (CrossRef Link)
[19] Ning T, Yang Z, Wu H, et al., "Self-Interest-Driven incentives for ad dissemination in autonomous mobile social networks[C]," in *Proc. of IEEE INFOCOM*, 2310-2318, 2013. Article (CrossRef Link).
[20] Boulis A, Srivastava M B, "Node-level energy management for sensor networks in the presence of multiple applications[C]," in *Proc. of the First IEEE International Conference on Pervasive Computing and Communications*, 41-49, 2003. Article (CrossRef Link).
[21] Shevade U, Song H H, Qiu L, et al., "Incentive-aware routing in DTNs[C]," in *Proc. of 2008 IEEE Inernational Conference on Network Protocols*, 238-247, 2008. Article (CrossRef Link).
[22] Zhou H, Chen J, Fan J, et al., "ConSub: Incentive-Based Content Subscribing in Selfish Opportunistic Mobile Networks[J]," *IEEE Journal on Selected Areas in Communications*, Vol. 31, no. 9, 669-679, 2013. Article (CrossRef Link).

[23] Mota V F S, Macedo D F, Ghamridoudane Y, et al., "A message-based incentive mechanism for opportunistic networking applications[C]," in *Proc. of IEEE Symposium on Computers and Communication (ISCC)*, 277-282, 2015. Article (CrossRef Link).
[24] He G, Debbah M, Lasaulce S, "Game theory for OFDM systems with incomplete information[J]," *Game Theory for Wireless Communications and Networking*, 2009. Article (CrossRef Link).
[25] Bigwood G, Henderson T, "IRONMAN: Using Social Networks to Add Incentives and Reputation to Opportunistic Networks[C]," in *Proc. of 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing*, 65-72, 2011. Article (CrossRef Link).
[26] Li Y, Yu J, Wang C, et al., "A novel bargaining based incentive protocol for opportunistic networks[J]," in *Proc. of 2012 IEEE Global Communications Conference (GLOBECOM)*, 5285-5289, 2012. Article (CrossRef Link).
[27] Wu J, Chen Z G and Zhao M, "Information cache management and data transmission algorithm in opportunistic social networks", *Wireless networks*, Vol. 25, no. 160, pp 1–12, 2018. Article (CrossRef Link).
[28] Lu X, Hui P, "An Energy-Efficient n-Epidemic Routing Protocol for Delay Tolerant Networks[C]," in *Proc. of IEEE Fifth International Conference on Networking, Architecture, and Storage*, 341-347, 2010. Article (CrossRef Link).

Haotian Wang is currently a master student of School of software, Central South University. He is also a researcher in ''Mobile Health'' Ministry of Education-China Mobile Joint Laboratory. His research interests include wireless communications and networking, wireless network.

Zhigang Chen received the B.E., the M.S. and Ph.D. from Central South University in China in 1984, 1987 and 1998. He is currently a Professor, Supervisor of Ph.D. and Dean of School of software, Central South University. He is also director and advanced member of China Computer Federation (CCF), and member of pervasive computing committee of CCF. His research interests cover the general area of cluster computing, parallel and distributed system, computer security, wireless networks.

Jia Wu received the Ph.D. Degrees in software engineering Central South University, Chang-sha, Hunan, P.R. China, in 2016. He is engineer in ''Mobile Health'' Ministry of Education-China Mobile Joint Laboratory and Post-doctor in School of information science and engineering Central South University. Since 2010, he has been Algorithm engineer in IBM company in Seoul, Republic of Korea and in Shang-hai, P.R. China. He is a senior member of CCF (China Computer Federation), a member of IEEE and ACM. His research interests include wireless communications and networking, wireless network, big data research, mobile health in network communication.

Leilei Wang is currently a master student of School of software, Central South University. She is also a researcher in ''Mobile Health'' Ministry of Education-China Mobile Joint Laboratory. His research interests include wireless communications and networking, wireless network.