Non-Cooperative Game Forwarding Leveraging User Trustworthiness in Mobile Edge Networks

Jirui Li 1,†, Xiaoyong Li 2,*,†, Guozhi Li 1 and Rui Zhang 3

1 School of Information Technology, Henan University of Chinese Medicine, Zhengzhou 450046, China; ljrokyes@163.com (J.L.); liguozhi@hactcm.edu.cn (G.L.)
2 Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing University of Posts and Telecommunications, Beijing 100876, China
3 School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tempe, AZ 85281, USA; rzhan100@asu.edu
* Correspondence: lixiaoyong@bupt.edu.cn
† These authors contributed equally to this work.

Abstract: Given frequent changes of network topology caused by limited computing power, strong mobility and weak reliability of most nodes in mobile edge computing (MEC) networks, a Non-Cooperative Game forwarding strategy based on user Trustworthiness (NCGT) is proposed to deal with low security and efficiency of data transmission. NCGT firstly considers device residual energy ratio, contact probability, service degree and link stability between devices to measure the reliability of nodes. Then, leverages Entropy Weight (EW) method and Golden Section Ratio (GSR) to develop a security optimal neighbors screening model based on multi-attribute decision-making, which ensures that high-performance security nodes are selected as forwarding game objects. Third, NCGT takes forwarding and non-forwarding as the policy set, designs the benefit function, and gets forwarding probability of nodes through Nash equilibrium, to reduce a large number of redundancy, competition and conflict in forwarding requests and improve its broadcasting efficiency. The simulation results show, NCGT is more effective against black hole and witch attacks than S-MODEST and AODV+FDG when there exists malicious nodes. Meanwhile, with the increasing of network load, NCGT with or without GSR always performs best in the terms of data delivery rate, delay, transmission energy consumption and system throughput in MEC environment.

Keywords: trustworthiness; non-cooperation; game theory; data forwarding; mobile edge networks

1. Introduction

As a new-type dynamic distributed self-organizing network, MEC network uses wireless access technology to services and cloud computing functions required by nearby telecom users, creating a telecom level service environment with high performance, low latency and high bandwidth, which will be widely used in civil, military and other fields [1]. The autonomous peer nodes in MEC networks use direct interaction to transmit data, and cooperate to process various services. However, the instability problems caused by high-speed movement of nodes, bandwidth and energy constraints of wireless links and malicious attacks, make the effective running of MEC networks more difficult than traditional distributed networks. Simply applying previous forwarding strategies to MEC networks will cause problems such as long query delay, high forwarding failure rate, and easy disclosure of privacy in the process of data transmission.

The higher the trust between nodes, the higher the security and success rate of data transmission, and the smaller the transmission delay. Thus, it is very necessary to select relays for MEC networks routing requests according to the trustworthiness between users. Social relationship of entity objects in real activities can evaluate the trustworthiness between them to a certain extent. Many social attributes, such as contact probability
between object nodes and nodal service degree, are usually used to measure the interaction strength between nodes when designing data forwarding models. That is because, the former reflects the interaction density between nodes and the latter reflects the reliability of a node, and using them can effectively resist the bad behavior of malicious or selfish nodes. The calculation of these social attributes can depend on different factors or methods such as contact times and duration [2] or Bayesian network [3] in different situations. Our previous studies [4,5] used “the frequency that node interact with one another” and “the success rate of node forwarding packets” to define contact probability and service degree, and built the trustworthiness forwarding models for mobile Internet of Things (IoT). Although these models can effectively improve the reliability of data transmission, the experiments existed a fatal flaw similar to other studies [2,3,6,7], namely, they did not consider the limitation of device energy and always held that all devices had enough energy for ever to transmit packets. In fact, with the operation of devices and the passage of time, their energy will gradually lose, some users with high trust maybe refuse to forward data because they need to use the remaining energy to do more important work or their devices are running out of energy. The literature [8] took device residual energy as one of the measurement factors of the trusted relationship between nodes, and combined contact probability and service degree to build a trustworthy forwarding model with energy constraints for mobile IoT. A large number of experimental results proved the necessity of applying node residual energy when designing forwarding schemes. However, it ignored a fact when selecting relay nodes, that is, all neighbor nodes of a node may be more distant from the target node than itself. Link stability prediction can effectively avoid packet transmission interruption caused by the above problem and reduce network overhead, which had been proved by existing studies [9,10]. To sum up, this paper will consider using contact probability, service degree, residual energy and link stability to build a trustworthy relationship measurement model between nodes for MEC networks.

Besides, a user carrying forwarded packets usually encounters multiple nodes with high trust and equivalent capability at a certain time. How to select optimal relays is the key to improve the success rate of data transmission and the operation performance of the system.

As one of the main methods of human behavior research, game theory plays a vital role in solving multi-user competition and designing well-organized security methodologies in the networks [11]. Generally, the game among multiple users includes cooperative game and non-cooperative game. The former refers to the existence of a binding agreement between the interacting parties, that is, a node needs to consider the decision results of other nodes when making decisions to achieve the best operation performance of the network. This makes cooperative game method not suitable for most MEC network data transmission decision-making scenarios. The main cause is, MEC network nodes move frequently and the contact time between nodes is usually short, and the high complexity of cooperative game will increase the decision-making difficulty of each node, resulting in low success rate of data transmission and too much data redundancy. On the contrary, non-cooperative static game will occupy a larger market in the instantaneous decision-making applications of MEC network multi-user game, because they do not have to consider each other’s decision-making results and can maximize personal interests. Meanwhile, on-demand forwarding protocols have attracted much attention at home and abroad because of its low routing overhead and no need to maintain the whole network information, and are widely used in MEC networks. The traditional on-demand forwarding protocols based on flooding mechanism are easy to lead to broadcast storm. To alleviate this problem, deterministic broadcasting scheme and probabilistic broadcasting scheme are proposed. The former selects a part of the nodes that receive broadcast packets to forward packets, and all nodes in the latter forward packets in a probabilistic manner. Compared with the former, the latter shows better robustness under the conditions of routing failure, network attack and dynamic topology. The key problem of probabilistic broadcasting scheme is how to obtain the forwarding probability of nodes? This is also one of the main problems
to be solved in MEC network forwarding model. Using the trustworthiness between nodes to calculate the forwarding probability is an effective way, which has been studied in literatures [2,4,5,8,11–13]. However, each forwarding judgment in the above research needs to compare and screen all neighbor nodes, which consumes node energy and channel bandwidth, but also increases the network overhead.

Therefore, to avoid forwarding data to nodes with lower trustworthiness and achieve the balance of node transmission capacity, link stability and overall network performance, a non-cooperative game forwarding scheme based on user trustworthiness (NCGT) is proposed in this paper. Its major contributions are shown as follows.

1. NCGT leverages node performance and social relations such as nodal residual energy ratio, contact probability, service degree and link stability, and EW method to objectively measure nodal trustworthy strength, which fundamentally ensures the reliability of relay node selection and the security of data transmission.

2. GSR (golden section ratio) is used to screen optimal game objects for each forwarding, which effectively improve the operation efficiency of NCGT model.

3. NCGT adds nodal trustworthiness in forwarding requests, takes forwarding and non-forwarding as game strategy set, and obtains node forwarding probability via Nash equilibrium, so as to reduce network redundancy, competition and conflict and improve forwarding efficiency.

4. NCGT is evaluated on a mixed network environment that includes the information from an analog network and one real dataset via comparing with S-MODEST [14] and AODV+FDG [11]. The simulation results show that NCGT has the greatest advantages in four aspects: cumulative delivery rate, average delivery latency, transmission energy consumption and system throughput.

The rest of the paper is organized as follows: Section 1 reviews the studies related to the theme of this paper. Section 2 introduces the measurement method of user trustworthiness based on multi-factor. In Section 3, we propose selection method of game objects and NCGT strategy, and design the rule and algorithm of NCGT model. Section 4 provides simulation parameters and the performance analysis for NCGT model. Section 5 briefly explains the existing problems and future work. We conclude this paper in Section 6.

2. Related Work

Data forwarding or routing and task computing offload [15] are the basic means for MEC network applications to achieve high efficiency and/or low energy consumption. Especially, with the rapid popularity of mobile devices, the allocation of network resources is separated from personal computing and gradually presented in the form of social interaction of mutual cooperation between people [16]. The explosive growth of social activities has led to bottlenecks in computing and communication, and has also greatly affected the quality of services provided by the network and the quality of customized delivered content. How to measure social relations and use them to build high credibility of interaction between nodes plays an important role in designing high efficient and/or low-energy data forwarding models [17,18] for MEC network applications.

Firstly, focus on the research related to the four trustworthy measurement factors between nodes selected in this paper. Bai et al., [3] leveraged Bayesian network to evaluate contact probability between nodes of delay tolerant network. The proposed estimation method has better performance in recall ratio and precision. Li et al., [19] calculated contact probability only using the number of contacts between nodes, and combined community structure to design forwarding model for social network. Dhelim et al., [20] proposed a context aware trust evaluation method to prevent the vehicle from being dangerous due to the transmission of false information and data in the vehicle Edge network. Hui et al., [2] modeled node centrality based on contact times and duration, and combined community relationship under real human flow trajectory to propose the famous Bubble Rap routing algorithm for delay tolerant network. Li et al., [4] leveraged social similarity and personal centrality based on contact probability and service degree to improve the trust between
nodes. Meanwhile, according to the actual operation of equipment, Klaiqi et al., [21] refined
and computed the energy consumption of devices when transmitting data in multi-hop
D2D communication network, and designed an adaptive routing mechanism to reduce the
network overhead. Wu et al., [22] used the residual and initial energy of sensor to assess
the impact of node energy consumption levels on forwarding scheme for wireless body
area networks (WBAN). Besides, Fu et al., [9] leveraged communication distance, physical
distance and relative translation velocity between devices to predict link stability from
source node to target node. Jiao et al., [23] predicted the link by using a training model
based on dynamic network sequence diagram sequence.

Although these studies had tried their best to enhance the trustworthiness between
nodes, the experiments may be inconsistent with the reality because of their idealization or
one-sidedness.

Secondly, focus on the research related to multi-user trustworthy game forwarding
in mobile networks. Mohammad et al., [11] combined AODV (ad hoc on-demand dis-
tance vector) [13] and node degree to raise a game-based probability forwarding strategy,
namely AODV+FDG, which performance was superior to AODV. Different from AODV,
DSR (dynamic source routing) [24] added its path information to the routing request pack-
ets, but it could not overcome the broadcast storm in the process of route discovery. To
detect the attackers accurately, enhance resource utilization and reduce system energy
consumption significantly, Kiran et al., [14] constructed a light weight routing security
strategy in IoT by using four models or theories such as non-cooperative game and specific
contextual trust evaluation. Balaji et al., [25] designed “an infinitely-repeated game and
cooperation approach” to identify malicious devices and improve energy-efficiency, how-
ever, the infinitely-repeated game increased time complexity. Wang et al., [26] proposed
“a game routing scheme for 3-D underwater acoustic sensor networks”, and but it existed
certain inferiority in term of average collision. Das et al., [27] combined “game-theoretic
and linear programming method” to put forward an adaptive intelligent energy-saving
routing strategy. The strategy only considered the solution from the perspective of lin-
ear programming constraints, and the amount of calculation is large. Huang et al., [28]
developed a game theory model to provide “optimal driving strategies for autonomous
vehicles under velocity control in the interior of a road link and route choice at a junction
node”. Qin et al., [29] leveraged game-theoretic to design a probabilistic routing model
to improve the enthusiasm of cooperation between selfish devices. The scheme did not
provide countermeasures against the phenomenon of gang deception in the network, and
could not effectively identify and shield malicious and aggressive nodes in forwarding.
Attiah et al., [30] developed “an evolutionary anti-coordination routing game model” to
solve the routing selection problem in a wireless sensor network. This model only analyzed
the fairness of the proposed equilibrium solution under the inaction of selfish nodes, and
did not verify the impact of malicious attacks.

The above research adopted various of methods or strategies to improve the efficiency
and reliability of game forwarding, however, the security and productiveness of data
transmission are not ideal because the credibility measurement method between nodes is
not perfect or the game group is not optimized in advance.

3. User Trustworthiness Measurement Based on Multi-Factor

This paper optimizes routing selection by comprehensively considering multiple
attribute factors in the process of packet forwarding according to the participating nodes’
own capabilities and network conditions, so as to ensure the reasonable allocation of system
resources. Therefore, this paper puts forward the following three basic requirements for
each node participating in forwarding.

• Ensure the reasonable utilization of node energy to increase the network life;
• Ensure the security of data transmission. Try to select nodes with high credibility to
  avoid potential network attacks such as eavesdropping, active attack and denial of
  service caused by malicious or selfish nodes;
• Ensure topology stability. Try to choose a path with strong link to reduce routing changes and network burden.

To meet the above requirements and ensure the efficiency of data transmission, this paper chooses four attribute factors closely related to nodes: residual energy ratio, contact probability, service degree [8] and link stability to measure the trustworthiness of participating nodes in packet forwarding. Obviously, each node has different attribute values and preferences when forwarding packets. Therefore, they can be set the corresponding values according to nodal actual situation, and this paper will give the definitions of the four factors referring to related studies [4,5,8,9].

Residual Energy Ratio. Assume \( RE_{ri} \) represents impact factor of residual energy of relay node \( r_i (i = 1, 2, \ldots, n) \), \( e_{ri} \) is the initial energy of \( r_i \), \( \Delta e_{ri} \) is all energy consumed by node to forward packets at a certain time, and then [8],

\[
RE_{ri} = \frac{e_{ri} - \Delta e_{ri}}{e_{ri}}
\]  

(1)

where \( \Delta e_{ri} = P^r_i D_{ri} \). \( P^r_i \) is the energy consumed by wireless links between \( r_i \) and other nodes to transmit unit bit data \( (J/\text{bit}) \), and \( D_{ri} \) is the amount of data passed by \( r_i \), and the two parameters are constants. Obviously \( 0 \leq RE_{ri} \leq 1 \). Note that when the residual energy of a node does not reach the preset threshold, it is not qualified to forward data.

Contact Probability. Nodal contact probability means its interactive frequency with other nodes in the network, which can be calculated based on contact times between devices. Note, this paper does not consider the real-time voice contact between devices. Suppose that \( c_{ri} \) is the number of contacts with node \( r_i \) in the network, and then its contact probability \( CP_{ri} \) is shown as follows [4,5,8],

\[
CP_{ri} = \frac{c_{ri}}{\sum_{i=1}^{n} c_{ri}}
\]  

(2)

Service Degree. In MEC networks, it can measure the reliability of node to forward data and effectively identify abnormal device nodes such as malicious or selfish [4,5]. Service degree \( SD(r_i) \) of \( r_i \) at a certain time is as follows.

\[
SD_{ri} = \frac{f_{ri}}{b_{ri}}
\]  

(3)

where \( f_{ri} \) represents the total number of packets successfully forwarded by \( r_i \), and \( b_{ri} \) is the total number of packets received by \( r_i \).

Link Stability. Predicting the link stability in advance can effectively avoid the transmission interruption caused by node movement or damage, so as to reduce the control overhead in the process of wireless transmission. Let \( LS_{ri} \) be the link stability, which is defined as follows referring to [9],

\[
LS_{ri} = \left[ \alpha \times \frac{d_{rg} - \min(d_{rg},dc)}{\max(d_{rg},dc)} + \beta \times \frac{v_{rd}}{v_{\max}} \right]^2
\]  

(4)

where \( g \) is the target node; \( d_{rg} \) and \( dc \) represent the geographical distance and the minimum communication distance between node \( r_i \) and \( g \) respectively; \( v_{rd} \) means the relative moving speed between \( r_i \) and \( g \); \( v_{\max} \) is the nodal maximum moving speed; \( \alpha \) and \( \beta \) \((\alpha + \beta = 1, 0 \leq \alpha, \beta \leq 1)\) are the weight coefficients that are obtained by referring to AHP analysis [31].

This paper first leverages the minimum distance \( \min(d_{rg},dc) \) and the relative moving speeding \( v_{rd} \) between \( r_i \) and \( g \) to build the judgment matrix of criterion layer in AHP, and each matrix element represents the scale value of the relative importance of the above two factors when compared. This paper subjectively sets the scale value of two factors with equal important as 1, sets the scale value that one factor is slightly, obviously, strongly and
extremely important than the other as 3, 5, 7 and 9 respectively, and takes 2, 4, 6 and 8 as the median value of the above adjacent judgment, while the scale value of the latter relative to the former is the reciprocal of the above value. Note, In the experimental part, in order to reflect the objectivity of the test results, the element values above the diagonal in the judgment matrix are randomly selected from 2 to 9 and their reciprocal set. The weight vector of criterion layer can be calculated by using the above judgment matrix. Second, the value of comparison matrix elements in the scheme layer of AHP follows the rule setting of the criterion layer, and the number of the comparison matrix depends on the number of links between \( r_i \) and \( g_{ij} \). The weight vector of the scheme layer can be obtained according to the above comparison matrix. Obviously, the number of elements in the weight vector is the number of links between \( r_i \) and \( g_{ij} \), and the number of sub-elements in each vector element is the number of factors in the criterion layer. Finally, the product of the weight vector in the scheme layer and the weight vector in the criterion layer is the calculated weight vector, that is, the weight vector composed of \( \alpha \) and \( \beta \) in Equation (4).

The core idea of multi-attribute utility method is to solve the problem of difficult comparison between different attributes. In this paper, each encounter node is required to submit a trustworthiness vector composed of different attributes that can be used to calculate its trustworthy value. Suppose \( T_{ri} \) denotes the trustworthiness value of node \( r_i \) at some time, and this paper defines it as follows.

\[
T_{ri} = \sum_{j=1}^{m} w_j A_{rij}
\]  

where \( w_j (0 \leq w_j \leq 1, \sum_{j=1}^{m} w_j = 1) \) is the weight coefficient and means the different importance of each attribute \( A_{rij} \) for measuring the trustworthiness of node \( r_i \). This paper adopts EW method \cite{32} to determine the weight of each attribute of node \( r_i \), and the information entropy of the \( j \)-th attribute of node \( r_i \) is calculated according to the following equation that is built referring to \cite{32}.

\[
EW_j = -(\ln n)^{-1} \sum_{r_i=1}^{n} p_{jr_i} \ln p_{jr_i}, \ j = 1, 2, \ldots, m
\]

In Equation (6), \( p_{jr_i} = A_{rij} \sum_{j=1}^{m} A_{rij} \), \( A_{rij} \) means the status value of the \( j - \)th attribute of the \( r_i - \)th relay node; \( n \) is the number of relay nodes in the efficient communication range of the node with forwarded packets; \( m \) is the number of attributes measuring relays performance. Therefore, the EW of the \( j - \)th attribute for relays can be gained based on Equation (7).

\[
w_j = \frac{1 - EW_j}{m - \sum_{j=1}^{m} EW_j}, \ j = 1, 2, \ldots, m
\]

The information entropy \( EW_j \) of an attribute is smaller, and its weight is bigger. On the contrary, the greater the information entropy of an attribute, the smaller its weight should be.

4. Trustworthiness-Based Non-Cooperative Game Forwarding Model (NCGT)

4.1. Selection of Game Objects

Because of nodal moving characteristic in MEC networks, the network topology is dynamic. When both the source node and the target node are determined at a certain time, what kind of node to choose as the relay will eventually affect the success rate, security and efficiency of packet delivery. Most of the previous studies used to calculate and compare the performance of all neighbor nodes of the current node carrying forwarding packets,
and then directly select the best one or select some nodes to participate in data transmission according to the artificially set proportion. They have two disadvantages. One is that the data transmission success rate may be reduced because the suboptimal relay nodes with more stable transmission path or more security may be screened out, and the other is that the experimental results will lose objectivity due to the human given screening ratio. Therefore, this paper first uses the nodal trustworthiness measurement in the Section II to evaluate all neighbors in the communication range of the current node with forwarding packets. Second, GSR in “optimization” [33] is leveraged to screen all neighbor nodes in the previous step to ensure the objectivity of each screening of forwarding nodes. Suppose that there are \( n' \) users in the forwarding at a certain time, the selection algorithm of game objects at this time is shown in Algorithm 1.

**Algorithm 1: Selection of Game Objects.**

<table>
<thead>
<tr>
<th>Input:</th>
<th>the node ( r_i ) with forwarding packets; user set ( V'' ); the related parameters of nodal trustworthiness measurement; the target node ( g ); GSR ( \psi );</th>
</tr>
</thead>
<tbody>
<tr>
<td>Output:</td>
<td>Game Objects set ( V ).</td>
</tr>
<tr>
<td>1</td>
<td>( V'' = \text{NULL}; V = \text{NULL}; n = 0; )</td>
</tr>
<tr>
<td>2</td>
<td>for each ( r_q (q \neq i) \in V'' ) do</td>
</tr>
<tr>
<td>3</td>
<td>Calculate ( RE_{r_q} ) according to Equation (1);</td>
</tr>
<tr>
<td>4</td>
<td>Calculate ( CP_{r_q} ) according to Equation (2);</td>
</tr>
<tr>
<td>5</td>
<td>Calculate ( SD_{r_q} ) according to Equation (3);</td>
</tr>
<tr>
<td>6</td>
<td>Calculate ( LS_{r_q} ) according to Equation (4);</td>
</tr>
<tr>
<td>7</td>
<td>Calculate ( T_{r_q} ) according to Equations (5)–(7);</td>
</tr>
<tr>
<td>8</td>
<td>end for</td>
</tr>
<tr>
<td>9</td>
<td>( V' \leftarrow \text{result of } V'' \text{ excluding } r_i \text{ in descending order of } T_{r_q}; )</td>
</tr>
<tr>
<td>10</td>
<td>( n = \lfloor n' \times \psi \rfloor; )</td>
</tr>
<tr>
<td>11</td>
<td>( V \leftarrow \text{the top } n \text{ neighbors in } V'; )</td>
</tr>
<tr>
<td>12</td>
<td>return ( V );</td>
</tr>
</tbody>
</table>

However, because the state of users may change at any time, the relationship between users may also change dynamically over time, and the game objects at different time may also change. The selection algorithm of game objects is based on the users’ state and interaction data, and does not calculate the participants in real time. The main causes include two aspects.

- In distributed computing environment, real-time computing will consume more computing resources.
- The user behavior is periodic [34], and the game objects also have the law of periodic change. Frequent user computing cannot significantly improve the performance of data transmission.

Therefore, to reflect the impact of users’ state and interaction changes on the game objects, this paper adopts the periodic update method to update the game objects’ information, and the update cycle is set by the system.

### 4.2. NCGT Strategy

In fact, NCGT is an on-demand routing strategy [35] that has attracted the attention of researchers at home and abroad because it has the advantages of low routing cost and does not need to maintain the whole network information. When the target node is not in the efficient range of the node with forwarding data, the latter will initiate the route discovery process. Similar to [35], NCGT regards data request forwarding process in route discovery operation as a multi-user non-cooperative game process. Namely, “the nodes involved in forwarding requests do not know the strategies of other nodes when making decisions, and there is no exchange of game information between the nodes involved in game forwarding.” Once a node makes a decision, it can no longer have any impact on the development of the game. Besides, because the dynamicity is a main characteristic of MEC networks, and the...
members taking part in forwarding data per time slot are different, the network changes with time. The paper defines $G = \{V, S, B\}$ as the network model at a certain time, where $V = \{r_1, r_2, \ldots, r_i, \ldots, r_n\}$ denotes the set of nodes participating in forwarding at a certain time; $S$ says the policy set that includes two elements: Forwarding ($F$) and Non-Forwarding ($NF$); $B$ is the profit function of node group forwarding game. Suppose that there are $n$ nodes who are the attendances of non-cooperative game forwarding at a certain time, and then choosing any one of them as the current node with forwarding packets, for example, $r_i$, and the strategy of node group game forwarding is shown in Table 1.

### Table 1. Forwarding Game Strategy.

<table>
<thead>
<tr>
<th></th>
<th>The Other $n-1$ Nodes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$r_i$</td>
<td>$F$ (When at Least One Node)</td>
<td>$NF$ (When All Nodes)</td>
</tr>
<tr>
<td>$F$</td>
<td>$b - b'$</td>
<td>$b - b'$</td>
</tr>
<tr>
<td>$NF$</td>
<td>$b$</td>
<td>$0$</td>
</tr>
</tbody>
</table>

In Table 1, $b \geq b' > 0$. Known from Table 1, when node $r_i$ chooses to forward data packets and the other $n-1$ nodes do not forward packets, or, when both $r_i$ and the other $n-1$ nodes do not forward packets, the profits of $r_i$ are $b - b'$. Meantime, when $r_i$ does not forward data and at least one of the other $n-1$ nodes chooses to forward packets, the profit of $r_i$ is $b$. However, when node $r_i$ and the other $n-1$ nodes all do not forward data packets, the profit of $r_i$ is 0. If one of the relay nodes forwards packets with probability $Y$, the probability that at least one of the other $n-1$ nodes forwards packets is defined in Equation (8) referring to [35].

$$Y_{n-1} = 1 - (1 - Y)^{n-1} \quad (8)$$

In the above group game forwarding, Nash equilibrium point is that the benefit when $r_i$ forwards packets is equal to the profit when $r_i$ does not forward packets and at least one of the other $n-1$ nodes forwards packets, and namely,

$$b - b' = b \times Y_{n-1} \quad (9)$$

Let $b = \Omega \times b'$, and $\Omega$ is a constant and $\Omega > 1$. After Equation (9) introduces $b$, it will transform into the form in the following.

$$Y = 1 - \Omega^{-\frac{1}{n-1}} \quad (10)$$

where, set $Y = 1$ when $n = 1$.

#### 4.3. NCGT Rule and Algorithm

Known from the above description, NCGT forwarding protocol is a non-cooperation forwarding strategy between users that is consistent with the characteristics that users do not know each other and do not discuss countermeasures in advance in real mobile edge networks. Moreover, this paper regards the trustworthiness of nodes as a key information in packet forwarding requests, and uniquely identifies a packet forwarding request by using the source node address and broadcast ID. In our NCGT model, the forwarding probability of packets is calculated via using Equation (10) closely related to node trustworthiness. The pseudo code of the NCGT strategy is shown in Algorithm 2.
Algorithm 2: NCGT Model.

**Input:** the node \( r_i \) with forwarding packets;
the target node \( g \);

```
BEGIN
V' = \{All neighbor nodes within the effective communication range of \( r_i \}\};
V = null; \( \text{rand} = 0 \);
for each \( r_j \in V' \) do
  if ((\( r_j == g \)) or (there are routes from \( r_j \) to \( g \))) and (\( r_j \) never received data to be forwarded)
    then \( r_i \) passes the data to \( g \) directly or through \( r_j \);
    jump to step 20;
  end for
V ← Algorithm 1 for \( V' \);
for each \( r_o \in V \) do
  Calculate \( Y \) according to Equations (8)–(10);
  \( \text{rand} = \text{Random()} \); // \( \text{Random()} \) is the random function.
  if (\( \text{rand} < Y \)) and (\( r_o \) never received data to be forwarded)
    then \{ obtain \( T_{r_o} \) by Equation (5);
    add \( T_{r_o} \) to the forwarded data;
    \( r_i \) forwards the data to \( r_o \);
    jump to step 1 and perform relevant operations on \( r_o \);
    \}
  end for
END
```

Obviously, at a certain time, a mobile device with forwarding packets needs judge its all neighbors \( V' \) within the effective communication range, and then transmits packets based on the following rules. First, traverse \( V' \) to find whether someone element of \( V' \) is or not the goal node or exists the path(s) to the goal node, and has never received the forwarding packets. If the above search result is true, the moving device with forwarding packets passes the data to the goal node directly or through the element node, and then ends the game. Otherwise second, leverage Algorithm 1 to gain optimal neighbor nodes set \( V \) of the current moving device. Third, traverse \( V \) to look for the adaptive neighbor node that can transmit forwarding packets to the goal node, and the corresponding operation includes the following three steps. (1) Calculate \( Y \) for each \( r_o \in V \) based on Equations (8)–(10); (2) Generate a random number between 0 and 1; (3) If the random number in step (2) is less than \( Y \) and \( r_o \) dose not receive the forwarding packets, the current moving device forwards the packets including \( T_{r_o} \) that is calculated by Equation (5) to \( r_o \) and then jump the start of this algorithm and re-perform the above operations on \( r_o \). Seen from Algorithm 2, its time complexity is related to the number of neighbors \( m \) of the moving device carrying the forwarding packets, which is \( O(m) \).

5. Performance Evaluation and Analysis

5.1. Simulation Settings

The experiments are executed in Matlab R2017b based on the environment with Intel(R) i5-4210 U CPU at 1.70 GHz 2.39 GHz, RAM 8 G, and 64 bits Windows 10 OS. To make the experimental results closer to the real scene, this paper considers using the hybrid experimental environment based on real-world network and analog network to evaluate the effectiveness of the NCGT model. We choose MIT Reality Mining dataset [36] based on human contacts as the real-world network. The dataset collected 1,086,404 Bluetooth interaction records of 100 users for about 9 months, and the interactive data of 85 users is regarded as the original data of the relationship between users after excluding some users with less data. Meanwhile, this paper builds an analog network which area is limited to 1000 * 1000 m², and randomly assigns coordinate positions to 85 users. In each experiment, both the source node and the goal node are randomly determined and are seen as normal nodes, and malicious nodes are also randomly selected from the remaining nodes.
in different proportions in order to reflect the randomness and uncertainty of malicious
nodes. Malicious nodes can simulate malicious acts such as Sybil Attacks via intercepting
or discarding data, and their cumulative delivery ratio (CDR) is set to 90% in the initial
stage of network operation to simulate malicious network attacks more realistically. The
experimental results are the average of all simulations, and Table 2 gives the name and
value of other parameters.

Table 2. Experimental parameters and values.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>packet size</td>
<td>50~100 KB</td>
</tr>
<tr>
<td>queue length on node</td>
<td>300~500</td>
</tr>
<tr>
<td>buffer size of node</td>
<td>5~10 MB</td>
</tr>
<tr>
<td>initial energy of node</td>
<td>19~100%</td>
</tr>
<tr>
<td>proportion of malicious nodes (%)</td>
<td>5, 15, 35, 60, 85</td>
</tr>
<tr>
<td>movement mode of node</td>
<td>random site moving model</td>
</tr>
<tr>
<td>maximum movement speed of node</td>
<td>6 m/s</td>
</tr>
<tr>
<td>data stream</td>
<td>CBR</td>
</tr>
<tr>
<td>data transmission rate</td>
<td>1 Mbps</td>
</tr>
<tr>
<td>communication radius of node</td>
<td>250 m</td>
</tr>
<tr>
<td>$p_r$</td>
<td>10 J/bit</td>
</tr>
<tr>
<td>simulation time</td>
<td>300 s</td>
</tr>
<tr>
<td>pause time</td>
<td>10 s</td>
</tr>
<tr>
<td>time to live (TTL)</td>
<td>5 h</td>
</tr>
</tbody>
</table>

5.2. Comparison Algorithms and Metrics

To validate the role of GSR for our NCGT strategy and the effectiveness of NCGT model
against black hole attacks, this paper compares with S-MODEST [14] and AODV+FDG [11]
with our NCGT model with and without GSR. S-MODEST is a lightweight routing security
strategy that integrated the DODAG-specific contextual trust model and RPL-specific rank
variance factor, in order to detect the attackers accurately and significantly reduces the
resource consumption. AVOD+FDG is a game-based probability forwarding scheme. It
used node degree information to gain the forwarding probability and apply it to AODV
protocol. The two forwarding models are both based on the classical forwarding algorithm
with social-aware properties, and are similar to our proposed model in some functions and
implementations.

Besides, this paper uses CDR, average delivery latency (ADL), transmission energy
consumption (TEC) and system throughput (ST) to measure the performance of all schemes,
which are redefined as follows in this paper.

(1). Cumulative Delivery Ratio CDR

$$CDR = \frac{PK_{received}}{PK_{sent}}$$ (11)

where $PK_{received}$ means the total number of packets successfully received by all goal nodes,
and $PK_{sent}$ is the total number of packets sent by all source nodes in the network.

(2). Average Delivery Latency ADL

$$ADL = \frac{1}{K} \sum_{\kappa=1}^{K} (R_{\kappa} - S_{\kappa})$$ (12)

where $K$ is the total number of packets successfully transmitted in the network, $R_{\kappa}$ repre-
sents the time when the $\kappa-th$ packet arrives at the goal node, and $S_{\kappa}$ denotes the time
when the $\kappa-th$ packet is sent.
(3) Transmission Energy Consumption TEC

\[ TEC = \sum_{i=1}^{n} \Delta e_i = \sum_{i=1}^{n} P_r^i D_r^i \]  \hspace{1cm} (13)

where the energy consumption of data calculation by device nodes is ignored, which main cause is that this paper focuses on the data transmission between mobile devices.

(4) System Throughput ST

\[ ST = \frac{1}{T_{\text{receive}} - T_{\text{send}}} \sum_{\kappa=1}^{K} R_{\text{bytes}}(\kappa) \]  \hspace{1cm} (14)

where \( T_{\text{send}} \) is the time when packets begin to be received in the system, \( T_{\text{receive}} \) is the time when the packet in the system ends receiving, and \( R_{\text{bytes}}(\kappa) \) means the bytes number of the \( \kappa - 1 \)th packet successfully reaching the goal node.

5.3. Results and Analysis

(1) Influence of Network Malicious Attack Intensity on Forwarding Performance

Changing the proportion of malicious nodes in the network can obtain the change of forwarding performance with network malicious attack intensity. This paper sets different proportion of the total number of nodes as the number of malicious nodes, and Figure 1 describes the performance comparison of all models under the changing number of malicious nodes when contracting rate of source node is 20%.

Figure 1. Performance comparison of all models in (a) Cumulative Delivery Rate, (b) Average Delivery Latency, (c) Transmission Energy Consumption and (d) System Throughput under different proportion of malicious nodes when contracting rate of source node is 20%.
Figure 1a shows the effect of network malicious attack intensity on CDR. Obviously, with the increasing of malicious node density, compared with the other two, our NCGT model performs best with or without GSR. The main cause is, NCGT model adopts the non-cooperative game forwarding strategy that is based on the trustworthiness between nodes measured by multi-interaction attributes. It focuses on the data forwarding ability and the stability of link between node pair, which ensures that the data will not be lost due to the change of network topology to the greatest extent. Therefore, it has better delivery capability. S-MODEST model can maintain the same path transmission after a transmission process. In this way, there is not only routing redundancy, but also nodes exit the network in advance due to excessive consumption of node energy, and the increase of malicious nodes will lead to data loss due to the increase of intermediate useless nodes. AODV+FDG model broadcasts Hello messages periodically, which leads to the increase of network conflicts and the decrease of cumulative delivery rate.

Known from Figure 1b, the ADL of all models increases with the increase of the number of malicious nodes in the network, and our NCGT model with or without GSR still is better than S-MODEST and AODV+FDG. It is because that the NCGT model uses the multi-trustworthiness factors between nodes to screen the forwarding neighbor nodes, and leverages the probability game to forward packets, which suppresses the network congestion, reduces the competition and conflict between nodes, and reduces the transmission delay.

Figure 1c shows the change trend of TEC of all models under different network malicious attack intensity, namely, the NCGT model has better energy characteristic than the other two and consumes less energy under the same proportion of malicious nodes. The cause is that our NCGT model leverages multi-trustworthiness attribute factors to make nodes play games to obtain the strategic equilibrium solution, avoid energy waste and have a longer life cycle than the other algorithms. S-MODEST model uses a single standard to select transmission nodes, which cannot clearly screen malicious nodes, and the problem of excessive energy consumption of nodes is prominent. AODV+FDG model requires nodes to broadcast Hello messages regularly, which increases the routing overhead.

Figure 1d exhibits that the throughput of all models changes with the intensity of malicious attacks. Although the ST of all models all decrease with the increase of the number of malicious nodes, the overall performance of our NCGT model is still the best. The NCGT mainly adopts multi-attributes-based trustworthiness analysis algorithm, applies non-cooperative game method, does not rely on Hello messages to obtain nodal credibility, and has high delivery rate and delay performance. Therefore, compared with the other two models, it has superior system throughput.

(2) Influence of Network Load on Forwarding Performance

The change of forwarding performance with network load can be obtained by changing the contracting rate of source nodes. Figure 2 shows the performance comparison of all models under different contracting rate of source node when the proportion of malicious nodes is 5%.

Figure 2a shows the change of CDR with network load. Although the curve of S-MODEST model is close to that of our NCGT without GSR, the CDR of NCGT remains the best. When the contracting rate of source node is less than 40%, all curves show a trend of increasing first and then decreasing. The cause is that, with the increase of network load, the number of packets arriving at the target node increases gradually, and the network load increases exponentially, and but, the number of packets arriving at the target node does not increase as fast as the network load. When the contracting rate is greater than 40%, the CDR of all models decreases sharply. Its main cause is, all models broadcast routing requests easily lead to serious competition and conflict when network load increases sharply. In this case, the forwarding strategy of NCGT and not broadcasting Hello messages can alleviate the network performance.

Figure 2b describes the change of ADL with network load, and the two are obviously in direct proportion. The main cause is, the increase of network load leads to the intensification of network competition and conflict, the number of packet retransmissions increases
gradually, and the number of source nodes restarting the route discovery process increases, so the delay performance decreases gradually. For all that, our NCGT still performs best, which cause is that it adopts probability forwarding strategy and does not need nodes to send Hello messages periodically, so as to alleviate the network congestion in this case.

Figure 2c exhibits the change of TEC with network load. When the contracting rate is less than 40%, all curves almost overlap and the increase is not obvious. After that, the increase begins to increase sharply, and the performance is also quite different. It is caused by serious network competition and conflict caused by the increase of network load. The reason why our NCGT model performs best is that it alleviates the broadcast storm caused by broadcast routing requests in the process of route discovery and reduces the number of transmitted packets in the network.

Figure 2d shows that the ST of all models first increases and then decreases with the increase of network load. It is because, the number of packets in the initial network does not reach its optimal capacity, and the system can fully digest them. However, with the continuous increase of packets, the network load becomes larger, the degree of network congestion intensifies, the resource competition is fierce, and the conflict is serious, resulting in the decrease of the number of packets reaching the target node and the decrease of system throughput. Meanwhile, the reason why our NCGT model performs best in this case is similar to that of TEC.

Besides, seen from the above experiments, NCGT model with GSR has better performance than that without GSR, which fully shows the positive effect of GSR and the necessity of its existence in NCGT.

Figure 2. Performance comparison of all models in (a) Cumulative Delivery Rate, (b) Average Delivery Latency, (c) Transmission Energy Consumption and (d) System Throughput under different contracting rate of source node when the proportion of malicious nodes is 5%.

6. Discussion

The proposed NCGT scheme tries its best to reduce the impact of network malicious behavior on data forwarding performance via leveraging multi-attribute based user trustworthiness and the high-performance non-cooperation game algorithm. Compared to the
other two models, all performance figures and numerical results have proved the accuracy and effectiveness of the proposed NCGT scheme. Nevertheless, NCGT does not provide an accurate method to identify malicious or selfish nodes, nor does it set a reward and punishment mechanism for participating nodes. Moreover, NCGT performs generally in the network environment with uneven node distribution, and needs to be further improved. These above deficiencies will be considered to solve in future work.

7. Conclusions

To reduce the impact of malicious attacks and selfish behavior on data transmission performance in MEC networks, this paper first constructs the corresponding calculation model for the trustworthiness strength measurement of relay nodes based on multiple trust attributes between nodes, and then uses GSR to preliminarily screen the game objects to improve the calculation efficiency of NCGT model. Finally, according to the characteristics of prior mutual ignorance of decision-making among mobile network nodes, a non-cooperative game forwarding strategy is designed to meet the real needs of the actual mobile networks. The experimental results prove that our NCGT can always achieve the best performance compared with S-MODEST and AODV+FDG in cumulative delivery rate, average delay, transmission energy consumption and system throughput.

Although NCGT has great advantages over the comparative models, its deficiencies and the characteristics of MEC network devices also determine that it still has a lot of room for performance improvement. Therefore, we plan to do two aspects of work to optimize the trustworthiness evaluation mechanism between nodes on the basis of preliminary research in the near future. One is to select or combine CPU, memory, WiFi and other factors that can better reflect the computing power and reliability of mobile devices as part of the measurement factors of trustworthy strength between nodes. The other is to try to provide a reward mechanism for normal devices to improve their enthusiasm to participate in forwarding, and build a punishment mechanism for abnormal nodes to reduce the probability of participating in forwarding.

Author Contributions: Conceptualization and methodology, J.L. and X.L.; writing, J.L.; supervision, X.L.; data curation and validation, J.L. and G.L.; investigation and visualization, R.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Joint Fund of NSFC-General Technology Fundamental Research (grant number U1836215, X.L.) and the Key Scientific Research Projects in Colleges and Universities in Henan (grant number 21A520025, J.L.).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: The authors would like to appreciate the editors and the anonymous reviewers for their insightful suggestions to improve the quality of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations
The following abbreviations are used in this manuscript:

- MEC Mobile edge computing
- EW Entropy weight
- GSR Golden section ratio

References


5. Li, J.; Li, X.; Yuan, J.; Zhang, R.; Fang, B. Fog computing-assisted trustworthy forwarding scheme in mobile Internet of Things. *IEEE Internet Things J.* 2019, 6, 2788–2796. [CrossRef]


8. Li, J.; Li, X.; Yuan, J.; Zhang, R. An Energy-Constrained Forwarding Scheme Based on Group Trustworthiness in Mobile Internet of Things. *IEEE Syst. J.* 2022, 16, 531–542. [CrossRef]


13. Saini, T.K.; Sharma, S.C. Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept. *Ad Hoc Netw.* 2020, 103, 102148. [CrossRef]


36. Sarker, I.H. Behavminer: Mining user behaviors from mobile phone data for personalized services. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, Greece, 19–23 March 2018.