Anonymous data collection scheme for cloud-aided mobile edge networks

Anxi Wang a,c, Jian Shen a,b,*, Chen Wang a, Huijie Yang a, Dengzhi Liu a

a School of Computer and Software, Nanjing University of Information Science & Technology, Nanjing, 210044, China
b Guangxi Key Laboratory of Cryptography and Information Security, Guilin, 541004, China
c National Supercomputing Center in Wuxi, 214000, China

A R T I C L E   I N F O
Keywords:
Cloud-aided mobile edge networks
Anonymous data collection
Communication model
Path selection

A B S T R A C T

With the rapid spread of smart sensors, data collection is becoming more and more important in Mobile Edge Networks (MENs). The collected data can be used in many applications based on the analysis results of these data by cloud computing. Nowadays, data collection schemes have been widely studied by researchers. However, most of the researches take the amount of collected data into consideration without thinking about the problem of privacy leakage of the collected data. In this paper, we propose an energy-efficient and anonymous data collection scheme for MENs to keep a balance between energy consumption and data privacy, in which the privacy information of sensors is hidden during data communication. In addition, the residual energy of nodes is taken into consideration in this scheme in particular when it comes to the selection of the relay node. The security analysis shows that no privacy information of the source node and relay node is leaked to attackers. Moreover, the simulation results demonstrate that the proposed scheme is better than other schemes in aspects of lifetime and energy consumption. At the end of the simulation part, we present a qualitative analysis for the proposed scheme and some conventional protocols. It is noteworthy that the proposed scheme outperforms the existing protocols in terms of the above indicators.

1. Introduction

Nodes in a cloud-aided Mobile Edge Network (MEN) are deployed and organized into a system for monitoring private data in real time [1, 2], in which the performance of the network, due to the constraints of various conditions, will become worse along with the operation of the network. Therefore, how to design routing strategies for private data transmission in MENs is an urgent problem that needs more attention. Under the cooperation of each module, a sensor node which is treated as a whole works very efficiently by taking advantage of its modules [3]. When assigned to a network, the main function of a node is to monitor the area and transfer data. Nowadays, sensors are used in different domains, including military and civil areas [4]. We introduce some applications where nodes are used to sense privacy data for their further usage by cloud computing [5].

Military: Sensors are used to get the topography-related parameters in this application, such as the height of the mountain, the speed of water flow, the wind speed, temperature, humidity, pressure, etc. These important parameters are used to generate a map of the monitored area for further military usage. In addition, smart sensors can be used to get data about vibration caused by human motions to locate enemies in military confrontations.

Extractive industry: The MEN is particularly suitable for production and scientific research in the following areas, such as greenhouse monitoring, measuring of the growth of precious economic crops, high-quality grape breeding and production, etc., which can greatly help the development of farming and increase farmers’ income. Adopting MENs to build an automatic monitoring system in the agricultural environment and using a set of network equipment to complete data collection can effectively improve the degree of intensive agricultural production and scientific agricultural production [6].

Smart home: Sensors provide rich background information through continuous monitoring. It is expected not only to solve this problem, but also to greatly improve the quality and efficiency of medical care [7]. The MEN integrates such technologies as microelectronics technology, embedded computing technology, modern network, wireless communication and distributed information processing, and then can realize real-time monitoring of objects through various integrated microsensors. It is currently one of the hot-spots that involve multidisciplinary high-level intersections and highly integrated knowledge [8].

* Corresponding author.

E-mail addresses: anxi_wang@126.com (A. Wang), s_shenjian@126.com (J. Shen), wangchennuist@126.com (C. Wang), hjyang@126.com (H. Yang), liudzdh@126.com (D. Liu).

https://doi.org/10.1016/j.dcan.2019.04.001
Received 27 February 2019; Received in revised form 26 March 2019; Accepted 5 April 2019
Available online 11 April 2019
2352-8648/© 2020 Chongqing University of Posts and Telecommunications. Production and hosting by Elsevier B.V. on behalf of KeAi. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
In most cases, the ability of a single node is very limited. As a result, most people can not reach or do not want to reach the environment of the sensor network area. So once a network is deployed, it is impractical to replace the energy supply module of the node. Therefore, reasonable use of the node's limited energy has become an important direction of research on MENs. From the beginning of the MEN until now, scholars have designed a lot of secure routing protocols to collect data [9].

One of the most famous protocols is the Low Energy Adaptive Clustering Hierarchy (LEACH) [10], which is proposed by Heinzelman in 2000. In the LEACH, the nodes which act as Cluster Heads (CHs) are randomly chosen by a stochastic function. What's more, the path from the CH node to the Base Station (BS) has only a single hop. After this scheme, an improved method of the protocol has been proposed. The directions for improvement mainly include the following two types: reselecting CH nodes and rebuilding clusters or finding a multi-hop path routing from CHs to the BS [11].

In order to simplify the management of the local node routing table, an active choice routing protocol is proposed in which the source node takes the initiative to look for the relay node to realize a fast delivery of data packets. The relay node takes the responsibilities of compressing the data from the source node and forwarding the packets. In addition, the relay node is very close to the source node. The energy consumption of the source node is lower when a neighbor node rather than a non-neighbor node is chosen to forward the data. Basically, research on the multi-hop path from the CH nodes to the BS in the previous works aims to reduce the energy consumption of CH nodes. The energy consumption of communication between long-distance nodes is very large. If the CH node can find a relay node to be the forwarder, the energy dissipation rate of CH nodes will be reduced significantly. This will prolong the lifetime of the entire network. As is mentioned in Ref. [12], selecting inner nodes as relay nodes for data transmission between the source node and the CH node will not reduce the lifetime of the entire network. To sum up, finding the multi-hop path in the cluster plays an important role in prolonging the lifetime of the network and achieving energy efficiency. In addition, some researchers have designed some secure encryption schemes for network data by public-Key encryption [13], quantum encryption [14], and so on.

However, these multi-hop path-based routing protocols cannot protect the nodes on the path, including their location and other important information, which is the component of the network topology [15]. Hence, we argue in this paper that the energy conservation of CH nodes and the energy consumption of relay nodes in the network should also be given enough attention. The necessity of designing the proposed approach is shown below. First of all, the protocol is designed to be suitable for large network regions. There is a great possibility that the distance between the edge node and the CH node is very large. Second, it does not contradict the idea that the management of the local nodes is not contradictory, because the number of nodes in the cluster is far larger than that of CH nodes in the actual application. Finally, when it comes to increasing the number of clusters in the network, we hold that there is a threshold for the percentage of CH nodes. When the percentage is higher than the threshold, the network performance will be greatly lowered. Therefore, the increase in the number of clusters is unworthy. Through the above analysis, we think it is necessary and practical to design an anonymous data collection scheme for local nodes [16].

1.1. Our contributions

In this paper, we focus on the secure communication between the nodes within one cluster to make intra-cluster communication more efficient, because this method can provide a longer lifetime and a higher packet delivery ratio compared with direct communication. The most important part of the multi-path selection method is to select the most suitable relay node, which helps the source node transmit data packages to the destination node. In addition, the identities and other information of nodes on the path are hidden to resist network attacks. The main contributions of our work are reflected in the following three aspects.

- A distance-based internal layering method is proposed to allocate the nodes in one cluster onto different layers based on their distance to the CH node. Note that the nodes are allocated into different clusters based on their residual energy levels.
- A routing selection method that has three stages to reduce the number of communication is designed. In addition, the data collection operation is completed within the path selection method, which protects the privacy of source and relay nodes.
- A security analysis shows that the privacy of the path in the scheme is protected away from attacks. Moreover, performance analysis shows that the proposed scheme is better than other schemes in terms of the network lifetime and the packet delivery ratio.

1.2. Organization

The rest of the paper is organized as follows: in section 2, some similar protocols, such as ROAM, HMRP, are discussed. Our proposed scheme is described in detail in section 3, and the energy consumption model of the proposed scheme is presented in this section, too. In section 4, the performance evaluation of our protocol, as well as the comparison with other protocols, is presented. The conclusion is drawn in section 6, and future work is mentioned as well.

2. Related works

Data collection scheme has become a hot research topic in MENs as researchers endeavor to collect more data with the limited residual energy of nodes and prolong the lifetime of the network. The multi-path routing has the advantage of achieving load balancing and is more resilient to route failures. Researchers have put forward a lot of methods of multi-hop path selection based on mathematics knowledge, which can take advantage of the lower routing overhead, the shorter end-to-end delay and the alleviated congestion in comparison with single-path routing protocols. These protocols can be roughly divided into two types: active choice protocols and passive choice protocols.

Here are a few active choice routing protocols. The goal of designing a Gradient broadcast [17] is to improve the robustness of data transmission and solve the particular problem of the processing and linking errors of the non-reachable nodes. The biggest advantage of this protocol is that the data packet transmission is robust through the cooperation of nodes. At the same time, it will bring about some overhead caused by the redundant information. The HMRP uses the concept of clustering to construct a whole network. In the data transmission phase, each node only needs to find its own next-hop nodes without saving all of the path information. The DGR is suitable for sensor networks which have limited bandwidth and energy. The task of transmitting data packets to the BS through the multi-hop path is realized. The main signal transmitted in the DGR is video signal. In addition, the DGR adds the Forward Error Correction (FEC) code technology into the signal. This protocol can achieve high energy efficiency in the network and it can avoid network conflicts. The Directional controlled fusion [18] is a fusion algorithm for directional control. The main contribution of the algorithm is that it achieves a balance between data compression and network load. In addition to that, the multi-hop path achieves a balance between depth and breadth by setting a fusion factor.

Compared with the active choice routing protocol, the passive choice routing protocol is not dominant in the number of routing protocols. Several representative protocols are selected as follows: in the Label-based multipath routing [19], each path is tagged with a label message. Through a broadcast, the LMR can find several disjoint paths, while there are several links used to protect the path of the link. However, the overhead for finding the suitable paths could not be ignored. The Cluster-based multi-path routing [20] effectively combines the clustering algorithm and the multi-hop path algorithm, and tries to find the
multi-hop path through the use of a clustering network. By this method, the multiple-path selection is provided for the network, which reduces the cost of routing control and enhances the stability of the network. The multi-hop path is only composed of CH nodes. The transmission process uses the diversity coding technique M-for-N to split the data packets to reduce their sizes, which also leads to a serious problem because the packet error rate will be significantly higher compared with other protocols. The routing protocol [21] is a protocol standard proposed by the Internet Engineering Task Force (IETF) group, and the path selection algorithm is implemented based on the directed graph of the destination.

3. Anonymous data collection scheme

In this section, the design of the proposed scheme will be discussed in detail. What's more, the reasons why the scheme can improve the performance of MENs are given. Specifically, our scheme focuses on reducing energy consumption by using relay nodes to forward data to CH nodes. In a word, the proposed protocol pays more attention to the communication within a cluster to make full use of the residual energy of nodes in the cluster. We do not make further improvement on the protocols. The routing protocol [21] is a protocol standard proposed by the Internet Engineering Task Force (IETF) group, and the path selection scheme, and energy consumption analysis.

3.1. Clustering and layering scheme

The clustering and layering scheme is the premise of the multi-hop path selection algorithm. The first step in this scheme is clustering, which is also an important research area of MENs. In this paper, we use a clustering algorithm that is based on energy distribution to determine the CH node [22]. Then the CH node completes the final cluster establishment. Once the position of the CH node is determined, the whole cluster will be completed. All CH nodes in the network broadcast a set of information about the cluster. In fact, the information just indicates the location and ID of the CH node. The remaining nodes in the network determine which cluster they belong to according to the intensity of the received broadcast information. At the same time, a message is returned to the CH node. This message, the residual energy information of the node is included and the information about its distance to the CH node is included, too. This message is prepared for the next layering stage.

After the CH node selection and the step of building a cluster are completed, each node is assigned to a local cluster. The advantage of this is to facilitate the management of local nodes. As the whole cluster is thought to be one node from the point of the BS, the privacy of the node is also relatively high. Of course, in addition to the role presented in the first part, the role of the CH node is more than one. The following is mainly about how to set up appropriate layers according to the distance and energy information after the CH node receives the feedback information of other nodes in the cluster. It should be pointed out that the interval between each layer is not exactly calculated. First, the CH node finds its distance to the local farthest node and sets the distance as the maximum distance of the cluster. Then, the number of nodes in the cluster will be calculated according to their IDs. Finally, the CH node starts to layer according to the number of nodes and the value of the maximum distance. The CH node is selected according to the concentration point of the network energy. It is obvious that, compared with the CH node, the number of nodes that have the same distance to the BS is relatively large.

3.2. Path selection scheme

The next task is data transmission. Path selection problem should be considered in data transmission. The final results of this stage are shown in Fig. 1. In this paper, we use the active cluster path selection scheme. When a node needs to send data packets to the CH node, the node first looks for another node within the range of one hop transmission. The source node collects the layer ID and the corresponding distance of all nodes in this range. After all the preparations are completed, the node begins to select an appropriate relay node. The selected relay node has a common feature, that is, the ID number of the layer in the node is less than or equal to that in the source node. During the relay transmission, the data packet is transmitted to the CH node.

3.3. Data collection scheme

We draw lessons from the pipelined in-network compression scheme which was proposed to realize data compression. The basic idea of this method is to reduce energy consumption at the expense of high delay. In this paper, we collect the sensor data stored in the buffer of the relay node. Relay nodes combine the data packet in the buffer and the collected packets into a data packet and forward the packet to the next. Note that the relay node will encrypt the packet with the pre-distribution pair-key of the BS [24]. The packet in the buffer will be removed from the relay node after the relay node has transmitted the data packet to the next one. In addition, the path of data transmission is erased to protect the source node.

3.4. Energy consumption analysis

The node energy consumption is an important index to measure the performance of a routing protocol. The main parameters considered include: energy consumption on sending and receiving per unit bit data.
packet, packet size, transmission distance, etc. According to the design of the proposed scheme, the scheme is optimized on data packet size and transmission distance, so we choose a well-known model which is also presented in Ref. [25].

The value of \( d \) plays a very important role in the calculation of the energy consumption. We can use \( d_{\text{trans}} = \frac{D_k - D_{k-1}}{n} \) to calculate the value of \( d \). Then, we bring it into the energy model. The total energy consumption of source node \( S \) can be expressed in Eq. (1) as

\[
E_{\text{con}} = \sum_{i=1}^{k} e_{\text{source}} + \sum_{i=1}^{n} e_{\text{receiver}}
\]

\[
= \sum_{i=1}^{k} \left( e_{\text{source}} + e_i(D_k - D_{k-1})^y \right) + \sum_{i=1}^{n} e_{\text{receiver}} k
\]

To ensure the smooth and efficient operation of the network, we simplify Eq. (1) to find the minimum of energy consumption, which is shown as

\[
E_{\text{min}}^{\text{con}}(n) = (2n - 1)e_{\text{source}} + e_i(D_k - D_{k-1})^y
\]

Here we can regard the energy consumption as a function takes \( n \) as an independent variable. And through the derivation, we can easily get the extreme value. From the known mathematical knowledge, we already know that the extreme value of the function will appear when the derivative function equals to 0, so we can find the appropriate number of relay nodes. The result is shown in Eq. (2) as

\[
n_{\text{int}} = \frac{(a - 1)e_i}{(2e_{\text{source}})^{1/a}}
\]

Then, we take the second derivative of \( E_{\text{min}}^{\text{con}} \) with respect to \( n_{\text{int}} \). The corresponding optimal transmission distance \( d_{\text{int}} \) for node \( S \) is given by Eq. (3) as

\[
d_{\text{int}} = \frac{D_k - D_{k-1}}{n_{\text{int}}} = \left( \frac{2e_{\text{source}}}{(a - 1)e_i} \right)^{1/a}
\]

Next, the average communication distance of nodes in one cluster is computed. In this process, the distances between the two layers are used as the communication range of nodes. In our design of the protocol, the average transmission distance of the node can be expressed as the average of the difference between the two layers, in which \( d \) is the value of the average distance, \( i \) is on behalf of the ID number of each layer. We can find that the sum of the transmission distance is the maximum distance threshold of the most outer layer. The distance threshold is brought into \( d_{\text{trans}} = \frac{\Delta d}{n} = \frac{\sum_{i=1}^{y} d_{\text{layer},i}}{y} \), and the average distance is calculated to be 31.05 m.

For the non-layer routing protocol in the cluster, the average distance of the node transmission can be calculated by \( d_{\text{trans}} = \frac{\sum_{i=1}^{y} d_{\text{layer},i}}{y} \), in which \( G_i \) represents the number of nodes in each layer, \( d_{\text{layer},i} \) represents the maximum distance threshold for each layer. As the percentage of clusters in our protocol is set at 5%, the number of nodes in each cluster is 20. When we bring all the data into \( d_{\text{trans}} = \frac{\sum_{i=1}^{y} d_{\text{layer},i}}{20} \), we can calculate the average distance to be 91.70 m.

By analyzing the result of the equations, we can see that the average transmission distance of the nodes in our protocol is far less than that of the routing protocol without layering. This means that we can get from the simple mathematical analysis and the optimization of our protocol to reduce the transmission distance of the node.

The reduction in the size of the data packet is also very significant. It is similar to the previous optimization of the transmission distance. In our scheme, when a relay node receives a data packet from the source node, the relay node compresses the data according to the linear relationship between the time and space of the data. At the same time, its perceived data can also be added to the packet before transmission. This reduction in the number of packets is very good for network operation. In our design of the network, only the most internal nodes can communicate with the CH. That means data packets were reduced from 20 \( l_{\text{data}} \) to 2 \( l_{\text{data}} \).

The above analysis is concerned with the improvement of energy consumption. From the microscopic point of view, our protocol reduces the average transmission distance of nodes. From a macro perspective, the new protocol reduces the total number of packets transmitted over the network. To sum up, adding layering thinking into the cluster can reduce energy consumption of nodes. What’s more, this idea can prolong the network lifetime.

4. Performance evaluation

In this section, we begin to compare the performances of the proposed protocol and some traditional routing protocols. The comparison method which we use is simulating the performance of the three performance indicators defined in Section 3 by the simulator. To do our experiments, we use the internationally recognized routing protocol simulator NS 2 [26], the experimental version for the latest NS 2.35. The operating platform of the simulator is a popular issue in Linux Ubuntu 12.04. The protocols under the experimental comparison are mainly LEACH, LEACH-C, EECRP and our protocol. At the end of this part, we’ll use a qualitative analytic method to compare other multi-path routing protocols with the above four protocols.

4.1. Simulation parameters

In the simulation comparison section, the network covers a 1000 m x 1000 m rectangular area. One hundred nodes are deployed in the network area, and the deployment method is at random. Detailed parameters of the simulation are the same as those in Ref. [22].

4.2. Simulation results

The experimental results are shown in Figs. 2–4. Through an analysis of the output file of the four protocols, we draw a trend graph by gnuplot. Firstly, we analyze the most important performance parameter of the network: lifetime. Then we analyze the packet delivery ratio. Finally, the energy consumption of the network is to be analyzed.
Secondly, the speed of the nodes' death is compared. Note that the number of live nodes in our scheme is decreased almost linearly after the 600th round, while the numbers of surviving nodes in LEACH-C, LEACH and EECRP are reduced sharply after the 100th round, the 400th round and the 400th round, respectively. In particular, in LEACH and EECRP, the entire network can only last for 200 more rounds after the first dead node appears. Finally, the round at which all nodes die is studied. LEACH-C only runs 400 rounds. LEACH and EECRP can run about 600 rounds. It is worth noting that the proposed scheme can run up to almost 1400 rounds.

**The number of messages received by the BSs:** Fig. 3 shows the number of messages received by the BSs of different protocols. Note that the number of data packets collected at the BS of our scheme is greatly increased, which is almost three times as those of the other three protocols. In fact, there are two data compression operations. One is carried out at the relay node before sending the data to the next node, the other is carried out at the CH node after collecting all of the data in the cluster. In the other three protocols, the data compression is only carried out at the CH node after data packets are sent to the CH node. In a word, our scheme can monitor the network environment in a long time with higher efficiency.

**Energy dissipation:** As shown in Fig. 4, the energy consumption rate of our scheme is at a lower level compared with the other three protocols. Moreover, the other three schemes make improvements by designing the CH node selection scheme but ignore making changes in the multi-path data transmission scheme. So the energy consumption rates of these schemes are almost the same. The node energy supply module makes an outstanding contribution, which guarantees a longer network lifetime and a real-time full-range monitoring of the network with limited energy.

### 4.3. Comparison with the conventional protocols

The property comparison between our scheme and the conventional protocols is summarized in Table 1 in terms of life cycle, scalability, computation & communication overhead, path selection, location awareness, robustness and mobility. As shown in Table 1, the proposed scheme performs better in most aspects. Note here that, with static sensor nodes and single hop between the BS and CH nodes, our scheme is suitable for networks in which the sensor nodes do not need to change locations. Last but not least, it is very suitable for us to deploy it in huge sensor networks.

To present our conclusion more comprehensively, we have analyzed the experimental results in Subsection 4.2. The main indicators of the analysis are the energy consumed per round and the energy consumed by each data packet. It can be seen from the simulation results in Subsection 4.2 that, the energy consumed per round in LEACH-C, LEACH and EECRP are 0.4762 (J), 0.3448 (J) and 0.3086 (J), respectively, while the energy consumed per round in our scheme is only 0.1386 (J), only 30%–40% of the others. It is obvious that the proposed scheme can obtain a longer lifetime in the case of the same initial energy. In addition, as for the energy consumed by the transmission of each packet, the results are very similar to the energy consumed by each data packet, in which the energy consumed by each data packet in our scheme is just 30%–40% of those of other protocols. In other words, when the four protocols need to transmit the same number of packets, our scheme consumes much less energy than

---

**Table 1**

Comparison among protocols.

<table>
<thead>
<tr>
<th>Protocol Properties</th>
<th>LEACH</th>
<th>LEACH-C</th>
<th>EECRP</th>
<th>Our scheme</th>
<th>ROAM</th>
<th>HMRP</th>
<th>CBMPR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Life cycle</td>
<td>Long</td>
<td>Longer than LEACH</td>
<td>Longer than LEACH</td>
<td>Longest</td>
<td>Longer than LEACH</td>
<td>Longer than LEACH</td>
<td>Longer than LEACH</td>
</tr>
<tr>
<td>Scalability</td>
<td>Limited</td>
<td>Limited</td>
<td>Limited</td>
<td>Good</td>
<td>Limited</td>
<td>Good</td>
<td>Limited</td>
</tr>
<tr>
<td>Computation &amp; communication overhead</td>
<td>Setting up and maintaining Cluster</td>
<td>Setting up and maintaining Cluster</td>
<td>Setting up and maintaining Cluster</td>
<td>Setting up and Path routing</td>
<td>Selection</td>
<td>Selection</td>
<td>Selection</td>
</tr>
<tr>
<td>Path selection</td>
<td>Single hop</td>
<td>Single hop</td>
<td>Single hop</td>
<td>Multi-hop</td>
<td>Multi-hop</td>
<td>Multi-hop</td>
<td>Multi-hop</td>
</tr>
<tr>
<td>Location awareness</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Robust</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Good</td>
<td>Limited</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>Mobility</td>
<td>Fixed BS</td>
<td>Fixed BS</td>
<td>Fixed BS</td>
<td>Fixed BS</td>
<td>Fixed BS</td>
<td>Fixed BS</td>
<td>Fixed BS</td>
</tr>
</tbody>
</table>

![Fig. 3. The number of messages received by BSs of the four protocols.](image)

![Fig. 4. The total energy dissipation of the four protocols.](image)
other three protocols. In a word, from both the quantitative and qualitative performance analysis, we can conclude that the proposed scheme improves the network performance greatly.

5. Conclusions and future works

In this paper, we propose an anonymous data collection scheme for cloud-aided mobile edge networks, where a layered algorithm based on the energy density of the cluster and a data compression algorithm in relay nodes are utilized to solve the problem of multi-hop path selection. Simulation results show that our scheme can transmit a great number of data packets with very low energy dissipation so as to prolong the network lifetime.

In the future, the communication among nodes should be encrypted to protect data away from attacks. In addition, it is necessary to study how to design a secure data sharing scheme for network data on a cloud computing platform. We hope that our future work can perform well in terms of keeping data security and nodes’ privacy.

Conflicts of interest

The authors declare that they have no conflicts of interest in this work.

Acknowledgments

This work is supported by the National Key R&D Program of China under Grant No. 2018YFB0805000, the National Natural Science Foundation of China under Grant No. U1836115, No. 61922045, No. U1836115 and No. 61672295, the Natural Science Foundation of Jiangsu Province under Grant No. BK20181408, the State Key Laboratory of Cryptology Foundation, Guangxi Key Laboratory of Cryptography and Information Security No. GCIS201715, the CICAEET fund, and the PAPD fund.

References