A Secure Data Aggregation Strategy in Edge Computing and Blockchain-Empowered Internet of Things

Xiaoding Wang, Sahil Garg, *Member, IEEE*, Hui Lin, Georges Kaddoum, Jia Hu, and M. Shamim Hossain, *Senior Member, IEEE*

***Abstract*—With the rapid development of the Internet of Things (IoT), more and more data are generated by smart devices to support various edge services. Since these data may contain sensitive information, security and privacy of data aggregation has become a key challenge in IoT. To tackle this problem, a blockchain-based secure data aggregation strategy, namely (BSDA), is proposed for edge computing empowered IoT. Specifically, in order to restrict task receivers [i.e., mobile data collectors (MDCs)] to search and accept tasks, the block header is intergraded with a security label including task security level (SL) and task completion requirement. Accordingly, new block generation rules are developed to improve system performance in throughput and transaction latency. Furthermore, BSDA decomposes both sensitive tasks and task receivers into groups against privacy disclosure. On the other hand, a deep reinforcement learning method, the improved self-adaptive double bootstrapped deep deterministic policy gradient (IDDPG), is developed to design energy-efficient MDC routes under the constrains that the SLs of MDCs should be higher than the SLs of data aggregation tasks. Simulation results indicate that 1) as a privacy-preserving strategy, BSDA obtains high throughput and low transaction latency and 2) BSDA outperforms certain contemporary strategies in aggregation ratio and energy cost.**

***Index Terms*—Blockchain, data aggregation, deep reinforcement learning (DRL), edge computing, Internet of Things (IoT).**

I. Introduction

With the rapid development of mobile devices (e.g., smartphone, smartwatch, tablet, etc.), a tremendous amount of data are generated everyday in Internet of Things (IoT) [1]. These data are aggregated by workers [i.e., mobile data collectors (MDCs)] and further analyzed for industrial applications. In the data aggregation process, there are two main concerns that worth our attention. The first one is how to aggregate data without privacy disclosure. For example, task releasers, who post data aggregation tasks, cannot tolerate the leakage of sensitive information contained in the task. Therefore, they prefer to choose trustworthy workers to fulfill the task. Note that as integration of distributed ledger, smart contract, peer-to-peer network, and consensus mechanism, the blockchain [2] can provide reliable access control, secure storage, and distributed computation. That suggests the privacy concern should be addressed by applying blockchain to data aggregation task design, i.e., a deliberately modified blockchain can restrict workers to the tasks of certain security levels (SL) and completion requirements (CRs). The second concern is how to be energy efficient due to data aggregation may cost workers a significant amount of energy. That suggests the data aggregation route should be designed with less energy cost. As a distributed open platform, the edge computing [3], which has been widely used in smart grids, healthcare, smart home, etc, integrates computing, storage, and applications to provide edge intelligence services. Therefore, edge computing can offer high-performance calculation for energy-efficient route design. Although plenty of works have been proposed to achieve secure data aggregation, only a few of which consider both SL-based task classification and energy-efficient task fulfillment. In this article, we propose a blockchain-based secure data aggregation strategy (BSDA) for edge computing empowered IoT. The details of our contributions are listed as follows.

1) To prevent privacy disclosure, the security label, which consists of task SL and task CR, is integrated with the block header design such that task receivers are limited to search and accept tasks of the corresponding SLs and CRs. Furthermore, both of sensitive task decomposition and task receivers partition are developed against collusion attack.
2) To improve system performance, we introduce new block generation rules that allow the block to be

Manuscript received 25 June 2020; revised 11 August 2020; accepted 28 August 2020. Date of publication 11 September 2020; date of current version 8 August 2022. This work was supported in part by the National Natural Science Foundation of China under Grant 61702103 and Grant 61772008; and in part by the Deanship of Scientific Research at King Saud University, Riyadh, Saudi Arabia, through the Vice Deanship of Scientific Research Chairs: Chair of Pervasive and Mobile Computing. *(Corresponding authors: Hui Lin; Jia Hu.)*

Xiaoding Wang and Hui Lin are with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350117, China (e-mail: wangdin1982@fjnu.edu.cn; linhui@fjnu.edu.cn).

Sahil Garg and Georges Kaddoum are with the Electrical Engineering Department, École de technologie supérieure, Montreal, QC H3C 1K3, Canada (e-mail: sahil.garg@ieee.org; georges.kaddoum@etsmtl.ca).

Jia Hu is with the Department Computer Science, University of Exeter, Exeter EX4 4QJ, U.K. (e-mail: j.hu@exeter.ac.uk).

M. Shamim Hossain is with the Chair of Pervasive and Mobile Computing and the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia (e-mail: mshossain@ksu.edu.sa).

Digital Object Identifier 10.1109/JIOT.2020.3023588

2327-4662 © 2020 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.
See https://www.ieee.org/publications/rights/index.html for more information.

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.

generated without waiting for a fixed period of time such that transaction processing is greatly improved.

3) To achieve energy efficiency in MDC route design, a deep reinforcement learning (DRL) method, the improved self-adaptive double bootstrapped deep deterministic policy gradient (IDDPG), is developed under the constrain that the SL of each MDC should not be inferior to that of the task meanwhile the task completion condition of each MDC should be higher than the CR of the task. Compared with traditional DRL methods, i.e., deep Q-network (DQN) and DDPG, IDDPG enables deep exploration, enhanced stability, and convergence acceleration such that the highly energy-efficient MDC route is discovered.
4) The simulation results indicate that a) BSDA can effectively resist the impact of collusion attack; b) BSDA obtains a high throughput and a low transaction latency under various scenarios; and c) the aggregation ratio of BSDA is higher than contemporary data aggregation strategies with the requirement of a lower energy cost.

The remainder of this article is organized as follows. Related work is covered in Section II. We introduce the system model in Section III. The details of the proposed strategy BSDA are elaborated in Section IV. The experiments are presented in Section V. We conclude this article in Section VI.

II. Related Work

The data aggregation in edge computing empowered IoT has drawn a great attention with lots of work proposed.

In the data aggregation route design, convex hulls are employed by Abbas and Younis [4] as MDC route. In [5], RCR is proposed by shortening MDC routes further with relay devices. In [6], Delaunay triangulation is applied to locate hyperedges of the hypergraph as MDC route such that CISIL is designed. In [7], LEEF adopts greedy expansion and optimization for MDC load balance. In [8], the latency is efficiently reduced and the load balance is improved in star topology. In [9], the load balance is further improved by dividing MDC routes into triangles. In [10], MDC routes are built based on convex hulls and further shortened utilizing center of mass. On the other hand, the influence of the realistic environment are considered in energy cost. In [11], the energy cost is minimized by utilizing stochastic geometry. In [12], MDCs are deployed in a network of a large scale by applying dynamic clustering and routing-based technology. Senturk *et al.* [13] quantified terrain influence to locate MDC route for energy cost minimization. Wang *et al.* [14] deployed MDCs and relay devices for data aggregation in realistic environments. In [15], both obstacles and collision avoidance are considered in data aggregation.

Machine learning is employed in data aggregation. In [16], the problem of privacy-preserving data aggregation is investigated by Yu *et al.* in the context of cyber–physical social systems. In [17], the data aggregation rate is predicted by an radial bias function neural network (RBFNN) to design energy-efficient MDC routes. Toyoshima *et al.* [18] adopted a DQN to design an event distribution-based data aggregation system with the consideration of 3-D environment. In [19], reinforcement learning (RL) is utilized for data aggregation and energy-aware data analysis. In [20], the blockchain is integrated with the MDC route design utilizing a DRL-based strategy. However, the above strategies cannot achieve the tradeoff between aggregation ratio and energy cost.

The blockchain is considered as a new privacy protection tool [21] and thus it is employed to achieve privacy-preserving data aggregation. In [22], the anonymous nature of blockchain is applied to worker privacy protection in data aggregation. In [23], the CrowdBC, a decentralized framework based on blockchain, is proposed. Users are registered without true identity and sensitive information is encrypted and stored in distributed storage. In [24], security and privacy concerns are considered for electrical data collections in smart grid utilizing edge computing and blockchain techniques. In [25], a distributed cloud structure based on blockchain is designed with fog nodes empowered software-defined networking. However, these strategies cannot achieve different SL-based data aggregation due to traditional block header structure and block generation rules.

Although previous works can provide efficient data aggregation in edge computing empowered IoT, there are still two problems that remain to be solved: 1) how to accomplish secure data aggregation, i.e., each MDC is only allowed to search and accept the task under the constrain that the SL of the MDC should not be inferior to that of the task meanwhile the task completion condition of the MDC should be higher than the CR of the task and 2) how to achieve energy efficiency in data aggregation under such constrain. In this article, we propose a BSDA to address these problems.

III. System Model

A blockchain-based data aggregation model in an edge computing empowered IoT network is considered in this article. In this model, two entities task releasers and task receivers exist. Task releasers post data aggregation task set $\{n_i\}_{i=1}^{N}$, in which each task n_i has a particular SL SL_{n_i} and a CR CR_{n_i}. The set of MDCs $\mathcal{M} = \{\mathcal{M}_i\}_{i=1}^{M}$, who serve as workers in blockchain, are responsible for data collection and aggregation, in which each $\mathcal{M}_i$ has a specific SL $\mathrm{SL}_{\mathcal{M}_i}$ and a task completion condition $\mathrm{CC}_{\mathcal{M}_i}$. Note that the SL of the task is somehow related to the application scenario. For example, a military data collection task should be set to the highest SL, while the environmental data collection task might be set to a normal SL. For example, there are 100 SLs with the lowest one between 0 to 30, the normal one between 30 to 60, and the highest one between 60 to 100. In addition, if a worker insists on contributing reliable data and completing the task, then he/she will be rewarded with more credits. That suggests the worker could search and accept the task of a higher SL. The interaction between these two entities is shown in Fig. 1, where the task is first released through the frontend page and then posted to blockchain via API interface.

More importantly, a task n_i can be searched and accepted by an MDC $\mathcal{M}_i$ only if $\mathrm{SL}_{\mathcal{M}_i} \geq \mathrm{SL}_{n_i}$ and $\mathrm{CC}_{\mathcal{M}_i} > \mathrm{CR}_{n_i}$. Once a data aggregation task n_i is fulfilled, the aggregation ratio

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.

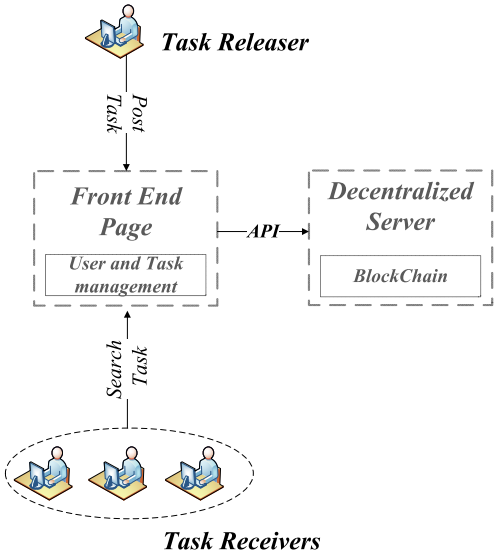


Fig. 1. Task releaser versus task receivers.

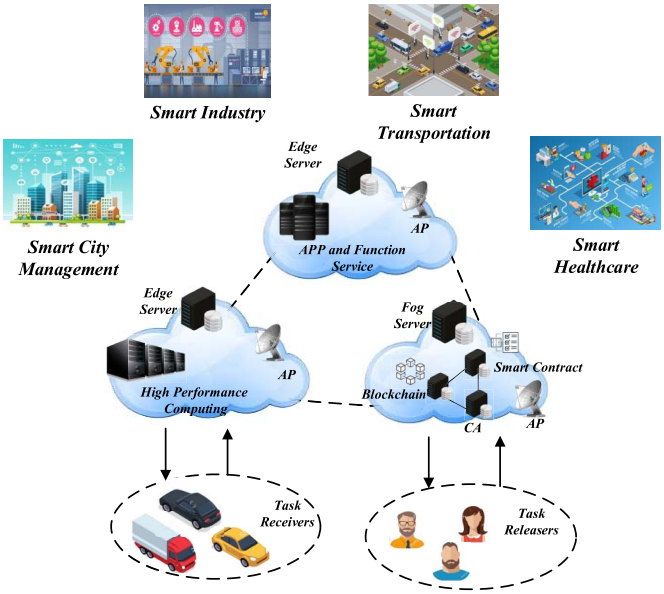


Fig. 2. System model of the BSDA.

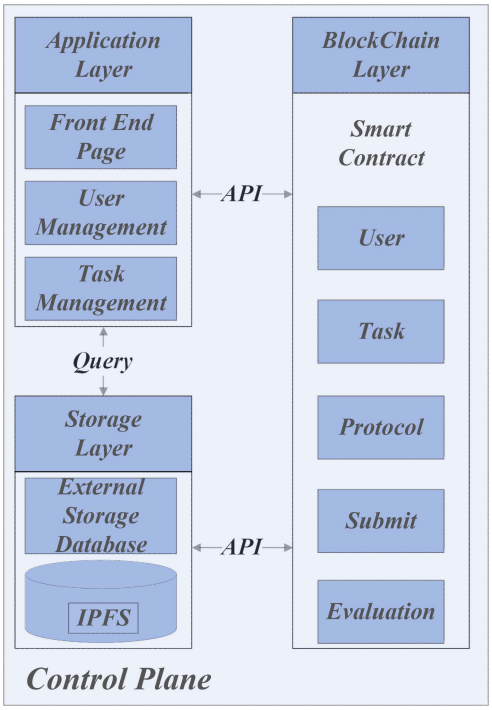


Fig. 3. Blockchain architecture of BSDA.

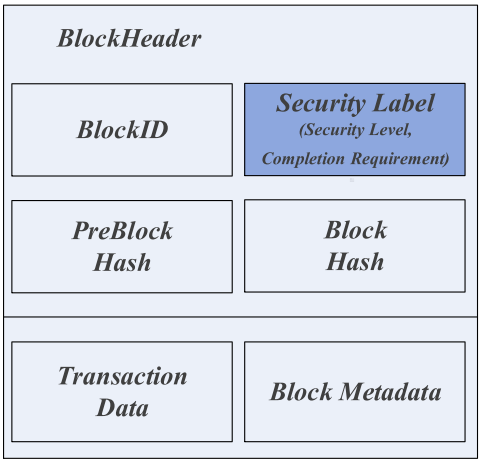


Fig. 4. Blockheader construction.

is applied for task assessment. In addition, we consider the energy efficiency is data aggregation. That suggests the MDC route design should ensure a high aggregation ratio and a low energy cost as well. Since edge computing can provide computational resources close to end devices that are connected to the network, edge servers are applied to both blockchain deployment and energy-efficient MDC route design. Fig. 2 gives the system model.

A. Attack Model

Note that once the posted tasks are accepted by task receivers, the collusion attack could cause privacy disclosure. For example, as an internal attack, the collusion attack is the one that task receivers collude with each other to share partial information to retrieve the complete sensitive information. In this article, we introduce security label-based header structure, sensitive task decomposition, and task receivers partition into the blockchain construction to resist collusion attack.

IV. Implementation Details of the BSDA

A. Security Label-Based Blockchain Construction

The blockchain architecture of BSDA is shown in Fig. 3. In this article, we aim to achieve the blockchain-based secure data aggregation with the consideration of both blockchain layer and application layer.

1) Blockchain Layer: When a task is released, BSDA call the smart contract to record relevant information and pack the task into a block as a transaction. To prevent the privacy disclosure, modifications have been made to the blockchain, i.e., the structure of block header is added a security label including the security level and the task CR as shown in Fig. 4

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.

Algorithm 1 Novel Block Generation

Initialize: A set of transactions
Ensure: New Block $B^{'}$

```
Task releaser posts task n_i
if SL_{n_i} ≥ SL_B then
    n_i is packed into the block B
end if
if BT_N > BT_Threshold or BS > BS_Threshold then
    Generate new block B'
end if
if preBlockHash, BlockHash, SecurityLevel and CompletionRequirement are verified then
    Block B' is added to blockchain
end if
```

to identify block SL. It follows that if a task n_i is packed into the block B, then the security of the task should reach that of the block, which is $\mathrm{SL}_{n_i} \geq \mathrm{SL}_B$, meanwhile the CR of the task should exceed that of the block, which is $\mathrm{CR}_{n_i} \geq \mathrm{CR}_B$.

For system performance improvement, block generation rules are designed with respect to both block size (BS) and the number of transactions (BT_N) in the block. Specifically, once the transactions are packaged in the block, if $\mathrm{BT}_N > \mathrm{BT}_{\mathrm{Threshold}}$ or $\mathrm{BS} > \mathrm{BS}_{\mathrm{Threshold}}$, then the block is added to the blockchain, where $\mathrm{BT}_{\mathrm{Threshold}}$ and $\mathrm{BS}_{\mathrm{Threshold}}$ represent the threshold of transaction and block size, respectively. In fact, the traditional block generation should wait for a period of time. Thereby, compared with the traditional block generation rule, BSDA allows blocks to be generated with the satisfaction of above rules such that the block generation is greatly accelerated. Furthermore, the processing capability of block transaction is significantly improved due to the acceleration of block generation. That suggests the new generation rules help the proposed BSDA to meet the requirements of data aggregation, i.e., throughput and transaction latency, in realistic applications. The novel block generation is summarized in Algorithm 1.

2) Application Layer: To solve the privacy disclosure problem, BSDA adopts both of sensitive task decomposition and task receivers partition. Specifically, once a sensitive task is released, it is partitioned into a set of subtasks, each of which only contains partial information. Therefore, it is difficult to obtain the complete sensitive information by getting only a part of it. However, if task receivers collude with others who accept different subtasks, then they still could recover the whole sensitive information by sharing their private parts. That explains why the system is still vulnerable to collusion attack if the task decomposition is the only resort. In fact, task receivers partition is an efficient resolution against collusion attack while collaborating with sensitive task decomposition. For example, a certain group of task receivers are only allowed to request the task assigned to this group for the avoidance of indirect privacy disclosure between different groups of task receivers. Besides, it is extremely difficult to find workers on other groups for task information sharing (see Fig. 5). Note that we adopt the secret sharing-based task decomposition, i.e., the sensitive information is divided into N "pieces" such

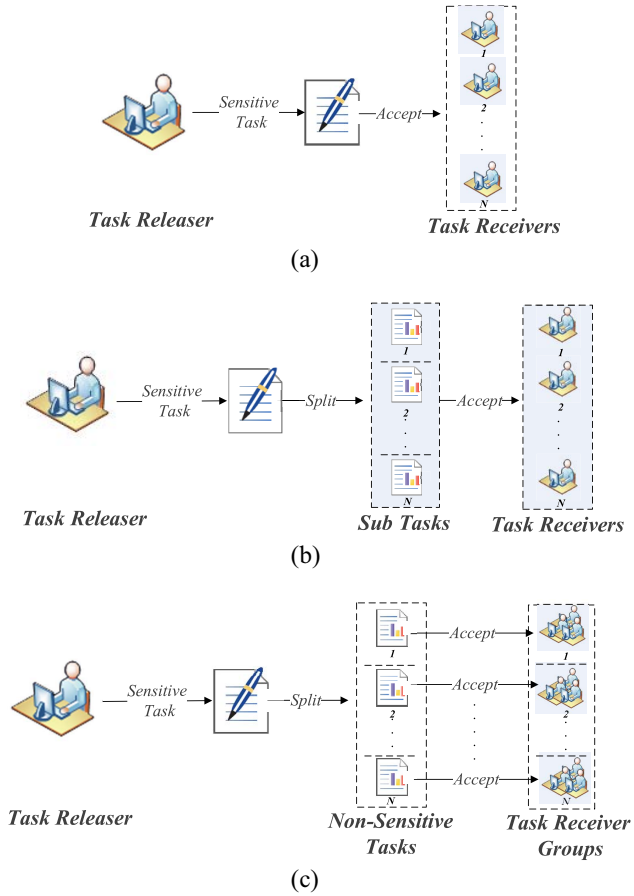


Fig. 5. Collusion attack prevention. (a) Sensitive information is accessible for each worker. (b) Sensitive information is recovered by collusion attack. (c) Sensitive information is preserved against collusion attack by task decomposition and task receivers partition.

that acquiring at least $N/2$ pieces can recover the whole sensitive information. We then give the theoretical proof on the capability of BSDA on collusion attack prevention.

Theorem 1: The proposed BSDA can efficiently prevent the collusion attack.

Proof: Let the area of tasks be denoted by s. Suppose there are λ task receivers per unit area. Since we adopt the secret sharing-based task decomposition, at least half of total N task receivers colluding with each other can recover the sensitive information. Let $\mathcal{N}(s)$ denote the number of task receivers on area s, while the probability of which $\mathcal{P}(\mathcal{N}(s) = n)$ is given by

$$\mathcal{P}(\mathcal{N}(s) = n) = \frac{(\lambda s)^n e^{-\lambda s}}{n!} \tag{1}$$

where $n = \lceil N/2 \rceil$. Thus, the probability $\mathcal{P}$ of n task receivers colluding with each other on area s is then given by

$$\begin{aligned} \mathcal{P} &= \frac{C_n^N}{N^n} \mathcal{P}(\mathcal{N}(s) = n) \\ &= \frac{C_n^N (\lambda s)^n e^{-\lambda s}}{N^n n!}. \end{aligned} \tag{2}$$

Then, taking the limit of $\mathcal{P}$ as $N \to +\infty$ yields

$$\lim_{N \to +\infty} \mathcal{P} = \lim_{N \to +\infty} \frac{C_n^N (\lambda s)^n e^{-\lambda s}}{N^n n!} = 0. \tag{3}$$

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.

The above equation indicates it is highly unlikely for half of task receivers to collude with each other such that the sensitive information would not be recovered. Thus, the proposed BSDA can efficiently prevent the collusion attack. ■

Although Theorem 1 proves the capability of the proposed BSDA against the collusion attack, task receivers could still compromise the task by contributing unreliable data. In this case, the SLs of corresponding task receivers should drop rapidly as the punishment for their actions. Accordingly, a softmax-based reputation management algorithm is developed as follows. We let $D_{\mathcal{M}_i}$ and C_{n_i} denote the data contributed by $\mathcal{M}_i$, and the credit for the task n_i, respectively. H_0 denotes $D_{\mathcal{M}_i}$ is reliable, while H_1 represents otherwise. Thus, the SL $\mathrm{SL}_{\mathcal{M}_i}$ is updated by

$$\mathrm{SL}_{\mathcal{M}_i} = \begin{cases} \mathrm{SL}_{\mathcal{M}_i} + C_{n_i} * \left(1 - \frac{e^{D_{\mathcal{M}_i} - \overline{D}}}{\sum_i e^{D_{\mathcal{M}_i} - \overline{D}}}\right), & \text{if } H_0 \\ \mathrm{SL}_{\mathcal{M}_i} - C_{n_i} * \frac{e^{D_{\mathcal{M}_i} - \overline{D}}}{\sum_i e^{D_{\mathcal{M}_i} - \overline{D}}}, & \text{if } H_1 \end{cases} \tag{4}$$

where $\overline{D}$ denote the authentic data of task n_i. With the help of above equation, the malicious task receivers can be prevented from searching and accepting the task of a high SL.

B. Energy-Efficient MDC Route Design With Security Level Constraint

1) Architecture of Improved Double Bootstrapped DDPG: Although machine learning technologies, i.e., deep learning (DL) [26] and RL [27], are efficient in discovering the optimal strategy, the energy-efficient MDC route design requires continuous space search on MDC moving directions. That indicates the traditional DRL (e.g., DQN and DDPG) are inefficient, i.e., DQN only performs well on discrete space, DDPG is subject to inefficient exploration and unstable training. To solve this problem, an IDDPG is developed for energy-efficient MDC route design. In fact, by introducing bootstrap to both actor and critic, the DBDDPG is developed [28] with a shared body and K randomly initialized heads $Q_{1:K}$ and $\eta_{1:K}$. It is worth to mention that the bootstrapped architecture requires less parameters and computation cost while training multiple models. Target networks of both critic heads (CHs) and actor heads (AHs), $Q'_{1:K}$ and $\eta'_{1:K}$, are updated slowly and stably as DDPG. The proposed IDDPG introduces new updating rules for both stability enhancement and convergence acceleration during the learning process.

For a DRL-based MDC route design, an MDC $\mathcal{M}_i$ of state $s_t^{\mathcal{M}_i}$ is given an action $a_t^{\mathcal{M}_i}$ at timeslot t such that $\mathcal{M}_i$ receives a reward $r_t^{\mathcal{M}_i}$ and the next state s_{t+1} observed from environment as well. Thus, the policy that can obtain the maximized reward should be discovered. In order to apply IDDPG to MDC route design, we first give the definitions of state, action, and reward, respectively.

a) State space: Each state s consists of two components, i.e., $s = (T, L)$. Be specific, T represents the set of tasks n_is of MDCs $\mathcal{M}_i$s, i.e., $T = \{n_i\}_{i=1}^{M}$ with $\mathrm{SL}_{\mathcal{M}_i} \geq \mathrm{SL}_{n_i}$; and L represents the locations of MDCs, i.e., $L = \{x^{\mathcal{M}_i}, y^{\mathcal{M}_i}\}_{i=1}^{M}$.

b) Action space: The action set A is composed of moving directions $\xi_t^{\mathcal{M}_i}$ and distance $d_t^{\mathcal{M}_i}$, i.e., $A = \{(\xi_t^{\mathcal{M}_i}, d_t^{\mathcal{M}_i})\}_{i=1}^{M}$.

c) Reward: The reward r_t is calculated using the data collected $\varphi_t^{\mathcal{M}_i}$ by timeslot t and energy cost E_T as

$$r_t = \sum_m r_t^{\mathcal{M}_i} \tag{5}$$

where

$$r_t^{\mathcal{M}_i} = \begin{cases} 0, & \text{if } \varphi_t^{\mathcal{M}_i} = 0 \\ \frac{\varphi_t^{\mathcal{M}_i}}{E_T}, & \text{otherwise.} \end{cases}$$

2) Ensemble Q-Value Evaluation and Q-Action Determination: If a state s_t is given by interacting with the environment, then potential action set $A_t = \{a_t^k\}_{k=1}^{K}$ is generated by K AHs. Meanwhile, Q value matrix $\phi_t \in \mathbb{R}^{K \times K}$ is constructed with respect to (s_t, A_t) by K CHs. Then, the weighted average on ϕ_t generated by the ensemble critic layer (E critic layer) gives rise to the ensemble Q value (EQ value), based on which the ensemble actor layer (E actor layer) determines the ensemble action (E action) a_t, i.e., the one with the maximum EQ value. That is

$$a_t = \arg\max_a \left\{ \sum_{i=1}^{K} \gamma_t^i Q_i\left(s_t, a | \vartheta_i^Q\right)|_{a=\eta_k(s_t|\vartheta_k^\eta)} \right\}_{k=1}^{K} \tag{6}$$

where γ_t^i denotes the confidence of critic head CH_i. Then, both state s_{t+1} and reward r_t are obtained by executing action a_t. The reason for introducing the structure of multiple critic–actor heads is that unreliable estimation made by a single critic will contribute to a poor action. That suggests if more than one critics make estimations, i.e., Q-values on state-action pairs, then it is more likely to discover the optimal action. Furthermore, Bernoulli distribution is utilized to generate a mask $m_t = (m^1, m^2, \ldots, m^K)_t$ randomly. This is because, in order to train each critic–actor head pair to achieve deep exploration, the data set that consists of transitions should be partitioned into subdata sets. By giving each transition a K bit binary representation with respect to Bernoulli distribution, it is convenient to assign each transition to a specific subdata set. Then, the experience pool stores the transition $(s_t, a_t, s_{t+1}, r_t, m_t)$. In this manner, different transitions sampled from experience pool are utilized to train different pair of AH and CH, i.e., the transition $(s_t, a_t, s_{t+1}, r_t, (1, 0, 0, \ldots, 0))$ can be only used to train the first pair of AH and CH. In addition, compared with the traditional DRL method, i.e., DDPG of the single actor–critic structure, the proposed IDDPG that consists of K AHs and K CHs are capable of generating one optimal action out of K action candidates. That suggests the generation of the optimal action is based on K separated subdata sets, each of which is carrying a specific mark m^i, $1 \geq i \geq K$, for deep exploration.

The training process of IDDPG employs the loss $\mathcal{L}(\vartheta_k^Q)$ to evaluate the performance of all CHs with a mini-batch transitions, each of which should carry a specific tag, i.e., $m^k = 1$, as

$$\mathcal{L}\left(\vartheta_k^Q\right) = \frac{1}{n} \sum_i \Big(r_i + \tau Q'\left(s_{i+1}, \eta'\left(s_{i+1}|\vartheta_k^{\eta'}\right)|\vartheta_k^{Q'}\right) - Q\left(s_i, a_i|\vartheta_k^Q\right)\Big)^2 \tag{7}$$

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.

where $\tau \in (0, 1]$ denotes the discount factor. For stability enhancement and convergence acceleration, the worst CH, i.e., the one of maximum loss given in (8), should be updated by minimizing the maximum square error (MSE) given in (7) through gradient descent

$$\mathrm{CH}_k = \arg\max_k \mathcal{L}\left(\vartheta_k^Q\right). \tag{8}$$

Accordingly, the kth AH is updated using policy gradient as

$$\nabla_{\vartheta_k^\eta} \leftarrow \frac{1}{n}\sum_i \nabla_a Q\left(s_i, a|\vartheta_k^Q\right)|_{a=\eta(s_i|\vartheta_k^\eta)} \nabla_{\vartheta_k^\eta}\eta\left(s_i|\vartheta_k^\eta\right). \tag{9}$$

Then, the target networks are updated by

$$\begin{aligned}\vartheta^{Q'} &\leftarrow \beta\vartheta^Q + (1-\beta)\vartheta^{Q'}\\ \vartheta^{\eta'} &\leftarrow \beta\vartheta^\eta + (1-\beta)\vartheta^{\eta'}\end{aligned} \tag{10}$$

with the learning rate $\beta \in (0, 1]$. Note that there exist K critic–actor head pairs with the same learning rate $\beta \in (0, 1]$. This is because the impact of unreliable estimation imposed by single critic–actor head pair is mitigated by introducing the structure of multiple critic–actor head pairs based on the same learning rate.

3) Self-Adaptive Confidence Module: It is worth to mention that the action selection depends on the Q value generated by CHs, which could be local optimal. That indicates the oscillation of the training process. The solution to this problem is to introduce the confidence mechanism, i.e., the confidence level of the ith CH, denoted by γ_t^i, to measure how confident the Q value evaluation is.

However, this method could raise the over confidence problem, i.e., CHs are always confident about the evaluation even if it is inaccurate. To address this problem, the self-adaptive confidence module (SACM), which is the actor network of parameter ψ with a single head and K outputs $\gamma_t = \{\gamma_t^k | \gamma_t^k \in (0, 1]\}_{k=1}^K$, is developed [28] utilizing dynamic weights adjustment, i.e., the positive reward improves the CHs' confidences while the negative one impairs CHs' confidences. Specifically, once the state s_t is observed from the environment, a confidence level γ_t^k is assigned to critic head CH_k. Then, both Q value matrix ϕ_t and confidence vector γ_t are applied to select the action with respect to EQ value on E critic layer. Eventually, the measurement of action and confidence of previous timeslot is implemented utilizing the reward r_t. Thus, the update of SACM by policy gradient on parameter ψ is then given by

$$\psi^C \leftarrow \psi^C + \alpha\nabla_{\psi^C} \log \pi_{\psi^C}(s_t, a_t) Q^\pi(s_t, a_t) \tag{11}$$

where $\alpha \in (0, 1]$ is the learning rate. Note that the above equation utilizes stochastic gradient to update SACM compared with actor networks updated using deterministic policy gradient. This is because SACM helps to find the optimal action by weighted evaluation on both E-critic layer and E-actor Layer such that the stochastic policy π is employed by SACM to generate K different weights. Accordingly, the reward r_t is chosen an unbiased sample of $Q^\pi(s_t, a_t)$. Thanks to the SACM, the learning process of IDDPG is stably improved. The framework of IDDPG is summarized in Fig. 6.

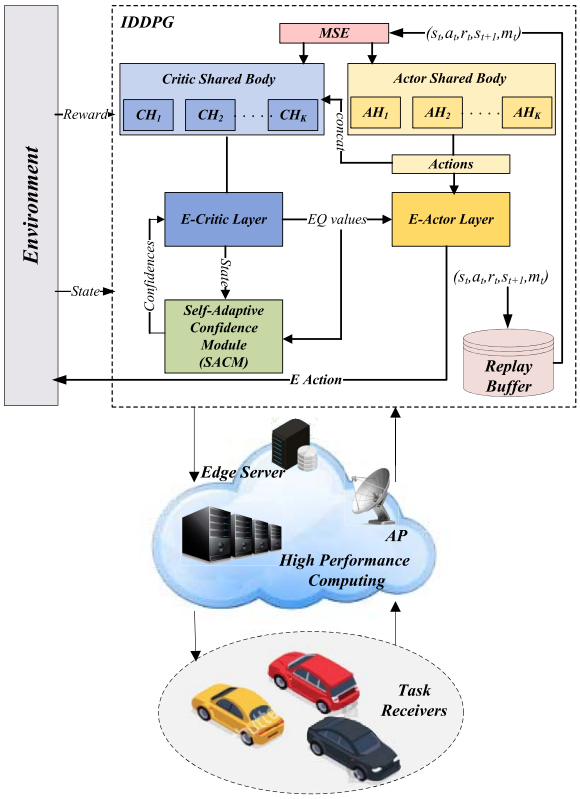


Fig. 6. Framework of IDDPG.

4) Exploration, Stability, and Convergence Analysis: IDDPG can achieve deep exploration, enhanced stability, and convergence acceleration.

1) *Deep Exploration:* IDDPG accomplishes subdata set-based parallel multimodel training with the help of the bootstrapped architecture. In addition, more potential actions search by AHs results in the diversity generalization in the learning process.
2) *Enhanced Stability:* Multicritic heads's weighted evaluation decides the output collaboratively rather than the unreliable estimation made by a critic only for accuracy improvement. That suggests IDDPG enhance stability by alleviating both uncertainty and degradation caused by a single critic-based decision.
3) *Convergence Acceleration:* The updating rule (8) adopted by IDDPG is to update the critic–actor head pair of the maximum bellman error [29] that can mitigate the impact of biased critics for convergence acceleration.

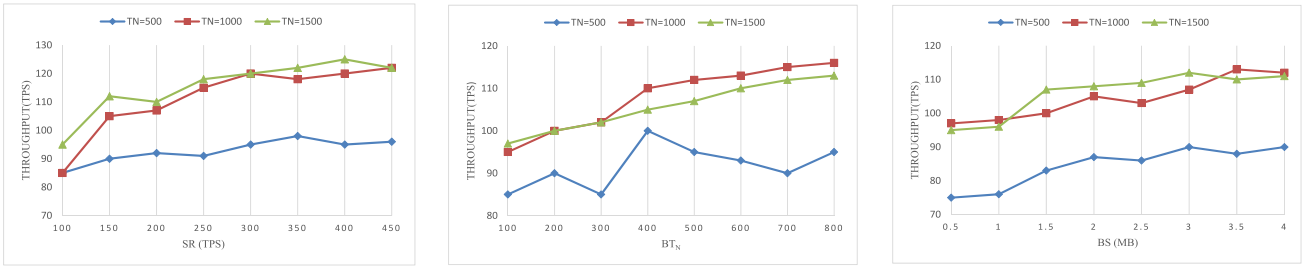
The MDC route design with IDDPG is summarized in Algorithm 2.

V. Performance Evaluation

A. Simulation Setup

In this simulation, a Hyperledger Fabric1.3-based simulator to implement the proposed strategy BSDA. The physical machine is equipped with Intel Core i7 processor, 16-GB running memory, CPU frequency 3.2-GHz 64-b win7 system, virtual computer software is the VMware Workstation 14 Pro,

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.



(a) (b) (c)

Fig. 7. Throughput of BSDA while varying (a) send rate (SR), (b) transaction number (BT_N) in block, and (c) block size (BS).

Algorithm 2 Energy-Efficient MDC Route Design With IDDPG

Initialize: head count K, distribution M of mask, critic and actor networks $\{\vartheta_k^Q, \vartheta_k^\eta\}_{k=1}^K$ and target networks $\{\vartheta_k^{Q'}, \vartheta_k^{\eta'}\}_{k=1}^K$, SACM ϕ^C, the maximum timeslot M.

for timeslot $t = 1, T$ **do**
  Choose action a_t via (6)
  Execute action a_t and calculate reward r_t via (5) then observe state s_{t+1}
  Sample bootstrapped mask $m_t \in M$
  Store $(s_t, a_t, s_{t+1}, r_t, m_t)$ in experience pool
  Sample transitions of a random mini-batch
  Update critic head Q^k via (7) and (8)
  Update actor head η^k via (9)
  Update target network k via (10)
  Update SACM via (11)
end for

TABLE I
EXPERIMENT SETUP

Para.	*Des.*	*Ran.*
N_R	Number of task releaser	3
N_M	Number of task receiver (i.e., MDC)	[5,12]
SR	Send rate	[100,450] tps
N	Number of data aggregation task	[100, 240]
T_N	Number of transactions to be processed	[500,1000,1500]
BT_N	Number of transactions in block	[100,800]
BS	Block size	[0.5,4] mb
r_c	Risk of terrains	(0,1]
V	MDC speed	[30,100] km/h
κ	Power constant coefficient	10^{-4} j/m^2
μ	Energy coefficient	25 j/m

the virtual machine is 8 GB of memory, allocated four processors, and 60 GB of Ubuntu system. We assume all tasks are located within 1000-m × 1000-m area of a TIN model. In addition, there are five realistic terrains, i.e., mountain, river, swamp, forest, and flat, considered in the validation experiment. We set the risk of each terrain is within the range (0, 1]. Table I gives the parameters of this simulation.

1) Performance Metrics: The performance of BSDA is validated by system throughput, transaction latency, and trusted task receiver selection rate (TSR) while varying T_N, SR, BT_N, and BS respectively. Then, BSDA compares with baseline approaches in aggregation ratio and energy cost while varying N_m, V, and N.

1) *Throughput:* A better system throughput suggests a higher transaction processing speed, which improves system performance.
2) *Transaction Latency:* A lower transaction latency indicates a better transaction processing capacity.
3) *Trusted Task Receiver Selection Rate:* The reputations of task receivers improve as *TSR* grows only if they complete tasks actively.
4) *Aggregation Ratio:* The proportion of data aggregated successfully to overall data, the aggregation ratio, is a key performance metric, i.e., a better data aggregation strategy should have a higher aggregation ratio.
5) *Energy Cost:* The energy cost in the data aggregation is a great concern such that reducing energy cost is crucial for energy-efficient MDC route design.
6) *Maximum Energy Cost:* The energy efficiency should consider the load balance. That suggests a better MDC route design will reduce the maximum energy cost.

We adopt the grid-based terrain quantification for energy cost calculation. Let r_c and d_c denote the distance and the risk, respectively. Then, the weight ω_c of cell c is given by

$$\omega_c = \int_{d_c} r_c. \tag{12}$$

For a route T, we then compute the energy consumption caused by terrain E_T^{Terrain} as

$$E_T^{\text{Terrain}} = \mu \sum_{c \in T} \omega_c \tag{13}$$

where μ represents the energy coefficient. On the other hand, the energy cost of data aggregation on task n_i by MDC $\mathcal{M}_j$, denoted as $E_{\mathcal{M}_j n_i}^{\text{Aggregation}}$, is determined by the power constant κ and the distance between $\mathcal{M}_j$ and task n_i, denoted by $d_{\mathcal{M}_j n_i}$, as

$$E_{\mathcal{M}_j n_i}^{\text{Aggregation}} = \kappa * d_{\mathcal{M}_j n_i}^2 \tag{14}$$

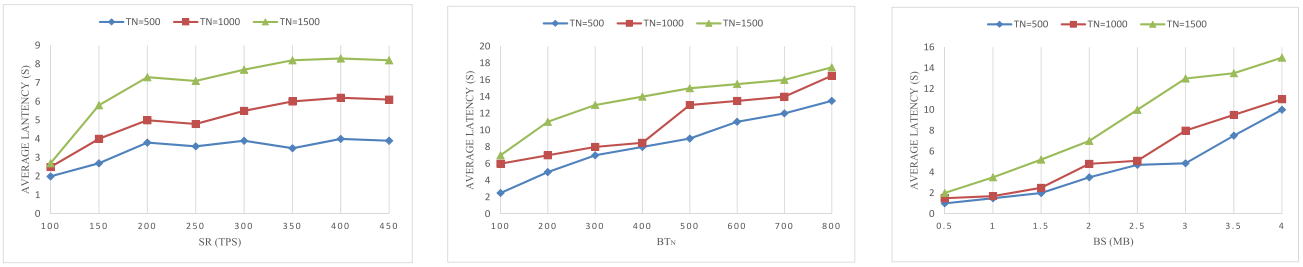
that suggests the overall energy cost along T, denoted by E_T^{MDC}, can be calculated as

$$E_T = E_T^{\text{Terrain}} + E_T^{\text{Aggregation}}. \tag{15}$$

B. Experiment Results

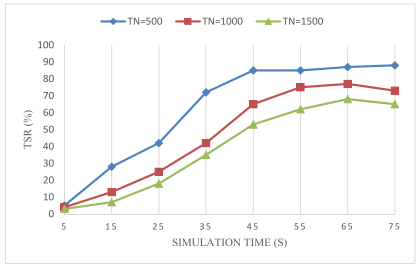
1) System Throughput: As shown in Fig. 7(a), it is clear that the throughput reaches 76, 92, and 96 tps, when T_N equals 500, 1000, and 1500, respectively. The system throughput changes

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.

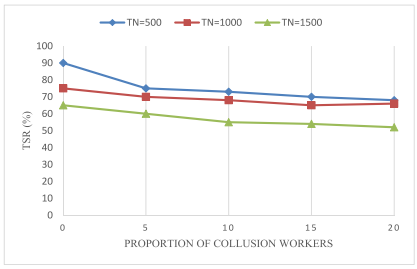


(a) (b) (c)

Fig. 8. Average latency of BSDA while varying (a) send rate (SR), (b) transaction number (TB_N) in block, and (c) block size (BS).



(a)



(b)

Fig. 9. Trusted TSR comparison (a) without collusion attack and (b) with collusion attacks.

slightly when $T_N \geq 500$ and stabilizes when SR $\geq$ 200 tps. Observed from Fig. 7(b) and (c), we know that the throughput does not continue to increase as either block size BS or number of transactions in block TB_N. When BS $\geq$ 3 MB or $TB_N \geq$ 600, the throughput begins to level off.

2) Transaction Latency: As shown in Fig. 8(a), the transaction latency increase with T_N. In addition, the transaction latency is less than 9 s if $T_N \leq 1500$. Once the send rate reach 200 tps, the transaction latency begins to level off. Thus, the send rate is set to 200 tps for block generation [see Fig. 8(b) and (c)] with the number of transactions TB_N in block and block size BS varying from 100 to 800 and 0.5 to 5 MB, respectively. It is obvious that the transaction latency increase with both block size and the number of transactions in the block.

3) Trusted Task Receiver Selection Rate: In Fig. 9(a), we know that as the simulation time goes *TSR* increases. The reason behind that is task receivers' reputations improve if they complete tasks without colluding with each other. As shown in Fig. 9(b), the increase of the proportion of collusion workers results in the dropping of *TSR*. Furthermore, as *TN* grows, *TSR* decreases first and stabilizes eventually.

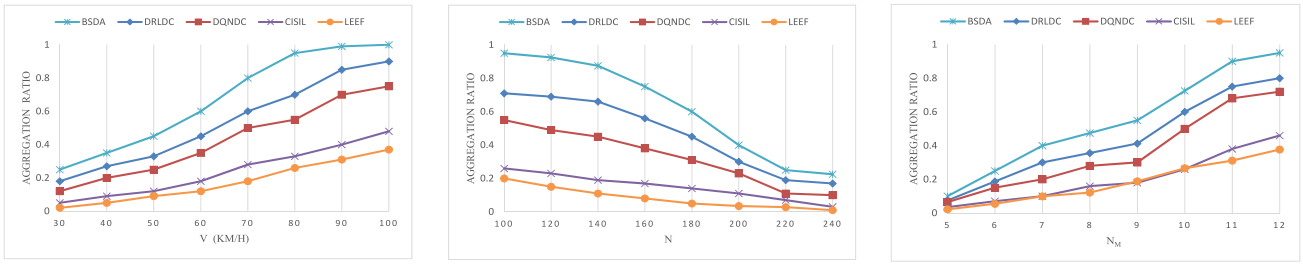
4) Aggregation Ratio: As shown in Fig. 10(a), as the speed V grows the aggregation ratio increases first and eventually levels off. BSDA has the highest aggregation ratio due to energy-efficient MDC route design. In Fig. 10(b), it is obvious that the aggregation ratio decreases as the number of task N increases for all approaches. The reason behind that is as follows. Although more tasks posted will result in data lost due to insufficient MDCs, the aggregation ratio will not constantly drops due to the reason that the area is densely populated with tasks. BSDA outperforms baseline approaches. In Fig. 10(c), it is obvious that as N_m grows, the aggregation ratio increases gradually first and stabilizes eventually. No doubt that BSDA beats all baseline approaches with the highest aggregation ratio.

5) Energy Cost: As shown in Fig. 11(a), it is clear that energy cost increases with the number of task N. BSDA requires the least energy cost among all baseline approaches. Note that the impact of velocity V on energy cost and MDC count N_M on maximum energy cost are shown in Fig. 11(b) and (c), respectively, with the number of data collection task $N = 240$. As shown in Fig. 11(b), the energy cost of each approach increases with V rapidly at the beginning and levels off eventually. This is because the faster an MDC travels the more energy cost is required meanwhile more data will be collected. Since the area of tasks is bounded, if the aggregation ratio reaches 100%, then no more data left to be collected such that no more energy will be consumed in data collection on tasks with respect to (14). That explains why the energy cost levels off rather than increase rapidly as the V. Observed from Fig. 11(c), we know that the maximum energy cost decrease as the number of MDC N_m increases with $N = 240$. In addition, BSDA not only has the least maximum energy cost but it is less affected by N_m as well.

VI. Conclusion

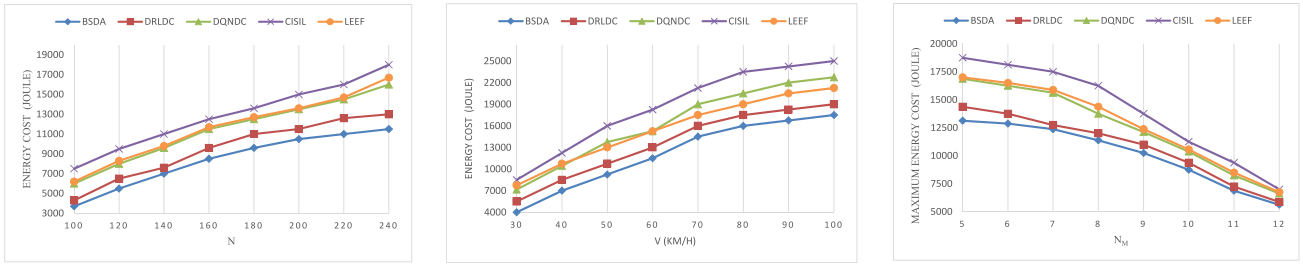
In this article, we propose a BSDA for edge computing empowered IoT. Specifically, all three important mechanisms, SL-based block header construction, sensitive task decomposition, and task receivers partition, are adopted by BSDA to prevent privacy disclosure. In addition, new block generation rules are introduced for transaction improvement. Furthermore, a DRL method, the IDDPG, is developed for energy-efficient data aggregation with the restriction on SL. The simulation

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.



(a) (b) (c)

Fig. 10. Performance comparison in aggregation ratio while changing (a) velocity V, (b) number of task N, and (c) number of MDCs N_m.



(a) (b) (c)

Fig. 11. Performance comparison in energy cost while changing in (a) number of task N, (b) MDC speed V, and (c) number of MDCs N_m.

results indicate that as an anti-collusion attack strategy, BSDA obtains a high throughput and a low transaction latency; meanwhile, compared with contemporary data aggregation strategies, the aggregation ratio of BSDA is higher and the energy cost is considerably lower.

REFERENCES

[1] R. Casadei, G. Fortino, D. Pianini, W. Russo, C. Savaglio, and M. Viroli, "Modelling and simulation of opportunistic IoT services with aggregate computing," *Future Gener. Comput. Syst.*, vol. 91, pp. 252–262, Feb. 2019.

[2] Q. Zhou, H. Huang, Z. Zheng, and J. Bian, "Solutions to scalability of blockchain: A survey," *IEEE Access*, vol. 8, pp. 16440–16455, 2020.

[3] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 62–67, Aug. 2018.

[4] A. Abbas, and M. Younis, "Establishing connectivity among disjoint terminals using a mix of stationary and mobile relays," *Comput. Commun.*, vol. 36, no. 13, pp. 1411–1421, 2013.

[5] Y. K. Joshi and M. Younis, "Restoring connectivity in a resource constrained WSN," *J. Netw. Comput. Appl.*, vol. 66, pp. 151–165, May 2016.

[6] W. Lalouani, M. Younis, and N. Badache, "Interconnecting isolated network segments through intermittent links," *J. Netw. Comput. Appl.*, vol. 108, pp. 53–63, Apr. 2018.

[7] S. Lee, M. Younis, B. Anglin, and M. Lee, "LEEF: Latency and energy efficient federation of disjoint wireless data collection position segments," *Ad Hoc Netw.*, vol. 71, pp. 88–103, Mar. 2018.

[8] J. L. V. M. Stanislaus and M. Younis, "Mobile relays based federation of multiple wireless sensor network segments with reduced-latency," in *Proc. IEEE Int. Conf. Commun.*, Budapest, Hungary, 2013, pp. 6407–6411.

[9] J. L. V. M. Stanislaus and M. Younis, "Delay-conscious federation of multiple wireless sensor network segments using mobile relays," in *Proc. IEEE Veh. Technol. Conf.*, Quebec City, QC, Canada, 2012, pp. 1–5.

[10] F. Senel and M. Younis, "Optimized interconnection of disjoint wireless sensor network segments using K mobile data collectors," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, ON, Canada, 2012, pp. 492–496.

[11] L. Goratti, T. Baykas, T. Rasheed, and S. Kato, "NACRP: A connectivity protocol for star topology wireless sensor networks," *IEEE Wireless Commun. Lett.*, vol. 5, no. 2, pp. 120–123, Apr. 2016.

[12] Z. Xu, L. Chen, C. Chen, and X. Guan, "Joint clustering and routing design for reliable and efficient data collection in large-scale wireless sensor networks," *IEEE Internet Things J.*, vol. 3, no. 4, pp. 520–532, Aug. 2016.

[13] I. F. Senturk, K. Akkaya, and S. Janansefat, "Towards realistic connectivity restoration in partitioned mobile data collection position networks," *Int. J. Commun. Syst.*, vol. 29, no. 2, pp. 230–250, 2016.

[14] X. Wang, L. Xu, S. Zhou, and W. Wu, "Hybrid recovery strategy based on random terrain in wireless sensor networks," *Sci. Program.*, vol. 2017, Jan. 2017, Art. no. 5807289.

[15] Z. Mi, Y. Yang, and J. Y. Yang, "Restoring connectivity of mobile robotic sensor networks while avoiding obstacles," *IEEE Sensors J.*, vol. 15, no. 8, pp. 4640–4650, Aug. 2015.

[16] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyber-physical social systems," *ACM Trans. Cyber Phys. Syst.*, vol. 3, no. 1, p. 8, 2018.

[17] J. Wang, H. Zhang, Z. Ruan, T. Wang, and X. D. Wang, "A machine learning based connectivity restoration strategy for industrial IoTs," *IEEE Access*, vol. 8, pp. 71136–71145, 2020.

[18] K. Toyoshima, T. Oda, M. Hirota, K. Katayama, and L. Barolli, "A DQN based mobile actor node control in WSAN: Simulation results of different distributions of events considering three-dimensional environment," in *Proc. Int. Conf. Emerg. Internetw. Data Web Technol.*, 2020, pp. 197–209.

[19] C. Xu, K. Wang, P. Li, R. Xia, S. Guo, and M. Guo, "Renewable energy-aware big data analytics in geo-distributed data centers with reinforcement learning," *IEEE Trans. Netw. Sci. Eng.*, vol. 7, no. 1, pp. 205–215, Jan.–Mar. 2020.

[20] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled data collection and sharing for industrial IoT with deep reinforcement learning," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3516–3526, Jun. 2019.

[21] M. Du, K. Wang, Y. Liu, K. Qian, Y. Sun, W. Xu, and S. Guo, "Spacechain: A three-dimensional blockchain architecture for IoT security," *IEEE Wireless Commun.*, vol. 27, no. 3, pp. 38–45, Jun. 2020.

[22] M. Yang, T. Zhu, K. Liang, W. Zhou, and R. H. Deng, "A blockchain-based location privacy-preserving crowdsensing system," *Future Gener. Comput. Syst.*, vol. 94, pp. 408–418, May 2019.

[23] M. Li *et al.*, "CrowdBC: A blockchain-based decentralized framework for crowdsourcing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 30, no. 6, pp. 1251–1266, Jun. 2019.

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.

[24] K. Gai, Y. Wu, L. Zhu, L. Xu, and Y. Zhang, "Permissioned blockchain and edge computing empowered privacy-preserving smart grid networks," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 7992–8004, Oct. 2019.
[25] P. K. Sharma, M. Y. Chen, and J. H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2017.
[26] Z. Chen, J. Hu, G. Min, A. Zomaya, and T. El-Ghazawi, "Towards accurate prediction for high-dimensional and highly-variable cloud workloads with deep learning," *IEEE Trans. Parallel Distrib. Syst.*, vol. 31, no. 4, pp. 923–934, Apr. 2020.
[27] J. Wang, J. Hu, G. Min, W. Zhan, Q. Ni, and N. Georgalas, "Computation offloading in multi-access edge computing using a deep sequential model based on reinforcement learning," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 64–69, May 2019.
[28] Z. Zheng, C. Yuan, Z. Lin, Y. Cheng, and H. Wu, "Self-adaptive double bootstrapped DDPG," in *Proc. 27th Int. Joint Conf. Artif. Intell.*, 2018, pp. 3198–3204.
[29] W. Shi, S. Song, C. Wu, and C. P. Chen, "Multi pseudo *Q*-learning-based deterministic policy gradient for tracking control of autonomous underwater vehicles," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 30, no. 12, pp. 3534–3546, Dec. 2019.

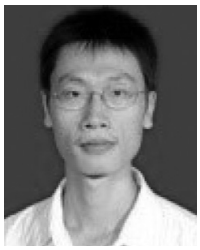
Xiaoding Wang received the Ph.D. degree from the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, in 2016.

He is an Associate Professor with the School of Fujian Normal University, Fuzhou. His main research interests include network optimization and fault tolerance.

Sahil Garg (Member, IEEE) received the Ph.D. degree from the Thapar Institute of Engineering and Technology, Patiala, India, in 2018.

He is currently working as a Postdoctoral Research Fellow with the Department of Electrical Engineering, École de technologie supérieure, Université du Québec, Montreal, QC, Canada. Some of his research findings are published in top-tier journals, such as IEEE TRANSACTIONS ON MULTIMEDIA, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING, IEEE INTERNET OF THINGS JOURNAL, IEEE NETWORK, *IEEE Communications Magazine*, *IEEE Wireless Communications Magazine*, *IEEE Consumer Electronics Magazine*, *Future Generation Computing Systems* (Elsevier), *Information Sciences* (Elsevier), and various international conferences of repute, such as IEEE Globecom, IEEE ICC, IEEE WCNC, IEEE VTC, IEEE Infocom Workshops, ACM MobiCom Workshops, and ACM MobiHoc Workshops. His research interests include machine learning, big data analytics, knowledge discovery, cloud computing, Internet of Things, software-defined networking, and vehicular *ad hoc* networks.

Dr. Garg was a recipient of the prestigious Visvesvaraya Ph.D. Fellowship from the Ministry of Electronics and Information Technology under Government of India from 2016 to 2018. For his research, he also received the IEEE ICC Best Paper Award in 2018. He serves as the Managing Editor for *Human-Centric Computing and Information Sciences* (Springer) and an Associate Editor of *IEEE Network Magazine*, IEEE SYSTEMS JOURNAL, *Applied Soft Computing* (Elsevier), *Future Generation Computing Systems*, and *International Journal of Communication Systems* (Wiley). He also serves as the Workshops and Symposia Officer for the IEEE ComSoc Emerging Technology Initiative on Aerial Communications.



Hui Lin received the Ph.D. degree in computing system architecture from the College of Computer Science, Xidian University, Xi'an, China, in 2013.

He is an M.E. supervisor with the College of Mathematics and Informatics, Fujian Normal University, Fuzhou, China, where he is a Professor with the College of Mathematics and Informatics. He has published more than 50 papers in international journals and conferences. His research interests include mobile cloud computing systems, blockchain, and network security.

Georges Kaddoum received the Ph.D. degree (with Hons.) in signal processing and telecommunications from the National Institute of Applied Sciences, Toulouse, France, in 2008.

He published over 200 journal and conference papers and two pending patents.

Dr. Kaddoum is a recipient of the "Research Excellence Award of the Université du Quebec, 2018" and the "Research Excellence Award-Emerging Researcher" from ÉTS, in 2019. He is a co-recipient of the Best Papers Awards of the IEEE PIMRC 2017 and the IEEE WiMob 2014. Moreover, he received the "Exemplary Reviewer Award" from IEEE TRANSACTIONS ON COMMUNICATIONS twice in 2015 and 2017. He is currently serving as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY and IEEE COMMUNICATIONS LETTERS. He held the ÉTS Research Chair in physical-layer security for wireless networks.

Jia Hu received the B.Eng and M.Eng. degrees in electronic engineering from Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2004, respectively, and the Ph.D. degree in computer science from the University of Bradford, Bradford, U.K., in 2010.

He is a Senior Lecturer of Computer Science with the University of Exeter, Exeter, U.K. He has published over 60 research papers within these areas in prestigious international journals and reputable international conferences. His research interests include edge-cloud computing, resource optimization, applied machine learning, and network security.

Dr. Hu has received the Best Paper Awards at IEEE SOSE'16 and IUCC14. He serves on the editorial board of *Computers and Electrical Engineering* (Elsevier) and has guest-edited many special issues in major international journals (e.g., IEEE INTERNET OF THINGS JOURNAL, *Computer Networks*, and *Ad-Hoc Networks*). He has served as the General Co-Chair of IEEE CIT'15 and IUCC'15, and the Program Co-Chair of IEEE ISPA'20, ScalCom'19, SmartCity'18, CYBCONF'17, and EAI SmartGIFT'2016.

M. Shamim Hossain (Senior Member, IEEE) received the Ph.D. degree in electrical and computer engineering from the University of Ottawa, Ottawa, ON, Canada, in 2019.

He is a Professor with the Department of Software Engineering, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia. He is also an Adjunct Professor with the School of Electrical Engineering and Computer Science, University of Ottawa. He has authored and coauthored more than 300 publications including refereed journals conference papers, books, and book chapters. Recently, he co-edited a book *Connected Health in Smart Cities* (Springer). His research interests include cloud networking, smart environment (smart city, smart health), AI, deep learning, edge computing, Internet of Things, multimedia for health care, and multimedia big data.

Prof. Hossain is on the editorial board of several SCI/ISI-Indexed Journals/Transactions, including the IEEE TRANSACTIONS ON MULTIMEDIA, IEEE MULTIMEDIA, IEEE NETWORK, IEEE WIRELESS COMMUNICATIONS, IEEE ACCESS, *Journal of Network and Computer Applications* (Elsevier), and *International Journal of Multimedia Tools and Applications* (Springer). He also presently serves as a Lead Guest Editor of IEEE NETWORK, *ACM Transactions on Internet Technology*, *ACM Transactions on Multimedia Computing, Communications, and Applications*, and *Multimedia Systems*. He is a Senior Member of ACM.

Authorized licensed use limited to: Fujian Normal University. Downloaded on June 13,2024 at 09:28:28 UTC from IEEE Xplore. Restrictions apply.