Endogenous Security of Computation Offloading in Blockchain-Empowered Internet of Things

Yiliang Liu
School of Cyber Science and Engineering
Xi'an Jiaotong University
Xi'an, China
liuyiliang@xjtu.edu.cn

Zhou Su
School of Cyber Science and Engineering
Xi'an Jiaotong University
Xi'an, China
zhousu@ieee.org

***Abstract*—This paper investigates computation offloading in blockchain-empowered Internet of Things (IoT), where the task data uploading link from sensors to small base station (SBS) is protected by intelligent reflecting surface (IRS)-assisted physical layer security (PLS). After receiving task data, the SBS allocates computational resources to help sensors perform the task. The existing computation offloading schemes usually focus on network performance improvement, such as energy consumption minimization, and neglect the Gas paid for computation offloading, resulting in the discontent of high Gas providers. Here, we design a Gas-oriented computation offloading scheme that guarantees the degree of satisfaction of sensors, while reducing energy consumption. Also, we deduce the ergodic secrecy rate of IRS-assisted PLS transmission that can represent the global secrecy performance to allocate computational resources. The simulations show that the proposed scheme has lower energy consumption compared to existing schemes, and ensures that the node paying higher Gas gets stronger computational resources.**

***Index Terms*—Internet of Things, blockchain, physical layer security, intelligent reflecting surface, Gas-Oriented.**

I. Introduction

With the rapid popularization of the Internet of Things (IoT) technologies in industrial manufacture, business, etc., the security issues of heterogeneous devices and infrastructures have raised many concerns. Building on their characteristics of decentralization, lightweight, and multimoding, the blockchain and physical layer security are regarded as enabling endogenous security technologies to address trust and confidentiality issues of IoT networks [1]–[4].

The typical application of blockchain-empowered IoT is the computation offloading of sensor nodes. Smart contracts record the offloading process participated by sensor nodes and mobile edge computing (MEC) servers onto the blockchain to ensure that transactions cannot be denied and malicious computing result providers will also be traced. However, the existing IoT computation offloading schemes have the following two challenges. Firstly, traditional schemes usually focus on the optimization of system performance, such as latency and energy consumption minimization [5]–[8]. The Gas factor just affects the block generation speed and is not considered in computational resource allocation, leading to the dissatisfaction of sensors because better computational resources are not allocated to those sensors even if they pay high Gas. Secondly, the security of links from the sensors to the MEC servers cannot be protected effectively because it is hard to establish secure communications based on cryptography technologies without the central trusted authority [9], [10]. In addition, due to the cost constraint of sensor devices, traditional PLS schemes, such as multiple-antenna beamforming or artificial noise technologies [11], are not suitable for IoT networks.

To address these problems mentioned above, we present Gas-oriented computational resource allocation to reduce energy consumption, while guaranteeing that the node paying higher Gas has more opportunities to get a stronger computational resource. The main contributions of this work are summarized as follows.

- We formulate the PLS-assisted computation offloading model in blockchain-empowered IoT, including phase shifter matrix adjustment and computational resource allocation to reduce the cost of energy consumption.
- We deduce the expression of optimal ergodic secrecy rate of IRS-assisted PLS channels, which provides a global metric of secrecy performance for computational resource allocation.
- We design a Gas-based computational resource allocation algorithm where sensors are divided into different groups based on paid Gas, and the group with higher Gas is prioritized with better computational resources.

The remainder of the paper is organized as follows. Section II describes the system model. The computation offloading scheme is proposed in Section III. We show simulation results in Section IV, and conclude this paper in Section V.

II. System Model and Problem Formulation

This article considers a blockchain-empowered IoT network, as shown in Fig. 1, which includes N_I sensor nodes, denoted by $\{U_1, U_2, ..., U_{N_I}\}$. Each sensor is equipped with one antenna. A set of N_K MEC servers, denoted by $\{M_1, M_2, ..., M_{N_K}\}$, are associated a single-antenna SBS via wired links, and $N_K \geq N_I$. All sensors and MEC servers are registered in a public Ethereum network and follow the rules of the Ethereum network. Due to the transmission power constraints and the large-scale fading effect of sensor communications, an IRS device is deployed to enhance the quality of the uplink channel from sensors to the SBS.

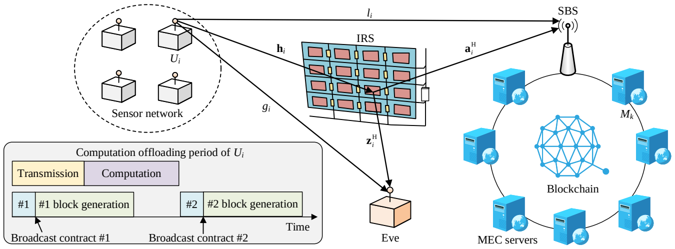

Fig. 1: Joint physical layer security and blockchain-assisted computation offloading in IoT networks

As the computational resources of sensors are scarce, these N_I sensors offload their computational tasks, denoted by $\{Z_1, Z_2, ..., Z_{N_I}\}$, to MEC servers via the wireless channels between sensors and the SBS. After receiving tasks, the SBS allocates virtual machines provided by MEC servers to execute these tasks. To record these tasks, sensors store the indices of publishing tasks on the Ethereum network via a contract function, i.e., $\mathsf{task\_publish\_contract}(\cdot)$, and the SBS stores the indices of results on the Ethereum network via the contract function $\mathsf{result\_record\_contract}(\cdot)$. Once the blocks of these contracts are deployed on the Ethereum network, none can repudiate the debts of transactions, and the results given by MEC servers are recorded to avoid the attacks of malicious MEC servers. The computation offloading process in the blockchain-empowered IoT network is described as follows.

1) Transmitting tasks to the SBS: U_i sends the task data to the SBS via IRS-assisted PLS schemes to resist eavesdropping attacks. To avoid the interference, sensors use the time-division multiple access (TDMA) technology during transmission processes.
2) Creating contracts of publishing tasks: At the same time of task transmission, by following the contract format of the Ethereum network, the sensor U_i launches a contract, i.e., $\#1 = \mathsf{task\_publish\_contract}(Z_i)$, which includes the hash message corresponding to the offloaded task Z_i and the signature of U_i. Also, the contract has the address information of the transaction parties[1], Gas for this transaction defined by V_i, Gas price[2], etc. Then, the contract $\#1$ is broadcast in the Ethereum network.
3) Computing tasks in MEC server: After receiving tasks, the SBS allocates computational resources of MEC servers to perform these tasks. It is assumed that a task uses one MEC server to compute results and an MEC server can be allocated to only one task. At last, the results are uploaded to the SBS for subsequent services.
4) Generating blocks of contracts of publishing tasks: All nodes in the Ethereum network synchronize the transaction of $\mathsf{task\_publish\_contract}(Z_i)$, and check its format and signature. If passing, nodes compete with each other to win the right of charging the account of the transaction, then the block is generated in the Ethereum network by winners. All members registered in the Ethereum network desiring to get payments can take part in the competition of account-charging rights.
5) Creating contracts of recording results: Without loss of generality, we assume that the task of U_i, i.e, Z_i, is offloaded to the MEC server M_k. After completing the task, M_k launches a contract, i.e., $\mathsf{result\_record\_contract}(Z_i)$, which includes the hash message of recording results, the signature of M_k, allocated computational resources, address information, Gas for this transaction, Gas price, etc.
6) Generating blocks of contracts of recording results: Similar to the block generation of contracts of publishing tasks, all members registered in the Ethereum network can take part in this competition of account-charging right. The winner can obtain Gas as a payment.

In this system, the IoT service acquirer should pay sensors and MEC servers because the original data is from sensors and data process is done by MEC servers. In this case, an IoT-enabled business model is established.

A. Communication Model

The article considers an IRS-assisted uplink communication model with a passive single-antenna eavesdropper (Eve). The IRS is equipped with N programmable phase shifter elements. All channels are assumed to obey Rayleigh fading. The channel from U_i to Eve is defined as $g_i \sim \mathcal{CN}(0, 1)$, the channel from IRS to Eve is defined as $\mathbf{z}_i^{\mathrm{H}} \sim \mathcal{CN}_{1,N}(\mathbf{0}, \mathbf{I}_N)$, the direct link from U_i to SBS is defined as $l_i \sim \mathcal{CN}(0, 1)$, the channel from U_i to IRS is defined as $\mathbf{h}_i \sim \mathcal{CN}_{N,1}(\mathbf{0}, \mathbf{I}_N)$, and the channel from IRS to SBS is defined as $\mathbf{a}_i^{\mathrm{H}} \sim \mathcal{CN}_{1,N}(\mathbf{0}, \mathbf{I}_N)$. The instantaneous CSIs of legitimate devices, including l_i, $\mathbf{h}_i$, and $\mathbf{a}_i^{\mathrm{H}}$, can be obtained via channel estimation perfectly, whereas the instantaneous Eve's CSIs g_i and $\mathbf{z}_i^{\mathrm{H}}$ are unknown. In this scenario, the TDMA technology is used, so inter-user interference is not existed.

For the security purpose, IRS controls programmable phase shifter elements via a phase shifter matrix, where the phase shifter matrix for the transmission period of U_i is defined as an $N \times N$ matrix $\mathbf{\Phi}_i$, i.e.,

$$\mathbf{\Phi}_i = \mathrm{diag}[\exp(j\theta_{i,1}), ..., \exp(j\theta_{i,n}), ..., \exp(j\theta_{i,N})], \quad (1)$$

and $\theta_{i,n} \in [0, 2\pi)$ is the phase introduced by the nth phase shifter element of IRS at the i-th period. With the phase shifter matrix $\mathbf{\Phi}_i$, the received signals at the BS and Eve can be expressed as

$$\mathbf{y} = \alpha_i (l_i + \mathbf{a}_i^{\mathrm{H}} \mathbf{\Phi}_i \mathbf{h}_i) x_i + n_i, \quad (2)$$

$$\mathbf{y}_{e,i} = \alpha_{e,i} (g_i + \mathbf{z}_i^{\mathrm{H}} \mathbf{\Phi}_i \mathbf{h}_i) x_i + n_{e,i}, \quad (3)$$

where $\mathrm{diag}(\mathbf{x})$ is the diagonal matrix of $\mathbf{x}$, α_i is the path loss between the SBS and U_i, $\alpha_{e,i}$ is the path loss between the SBS and Eve, x_i is the confidential information-bearing signal from U_i with $\mathbb{E}(|x|^2) = P_i$, and P_i is the transmission

[1] The sending address is related to U_i, and the received address is null as contracts of publishing tasks should be broadcast in the Ethereum network.

[2] Gas price has the unit ETH or Gwei. The fee of transaction can be calculated by Gas × Gas price. Gas price has a transformation to legal tenders. For instance, a transaction needs 100 Gwei with 6.5×10^{-7} dollar/Gwei.

power of U_i. n_i and $n_{e,i}$ are the additive white Gaussian noise (AWGN) obeying $\mathcal{CN}(0, \sigma_i^2)$ and $\mathcal{CN}(0, \sigma_{e,i}^2)$, respectively.

B. Energy Consumption Model

The sensor U_i has the computation task Z_i with D_i-bits data that should be uploaded to SBS. After receiving the task data, the SBS will select an MEC server, such as M_k, to perform the task of U_i. In this model, when D_i-bits data are calculated in M_k, the computing period is $c_k D_i / f_k$, where c_k (CCN/bit) is the CPU cycle number (CCN) per bit processing at M_k, and f_k (CCN/s) is the CCN per second of M_k. The energy consumption per second of M_k is $\eta_k f_k^3$ (Joule/s), where η_k is the computation energy efficiency coefficient of CPU chips in M_k. The transmission delay of uploading can be expressed as $D_i/(R_i B)$, where R_i (bit/s) is the ergodic secrecy rate of uplink channels, and B is bandwidth. The energy consumption of Z_i with the assistance of M_k can be formulated as

$$Q_{i,k} = \eta_k D_i c_k f_k^2 + \frac{D_i P_i}{R_i B}. \tag{4}$$

The computing modules of the Ethereum are worldwide distribution, and are independent of the computation offloading system, so the energy consumption of the Ethereum network is not considered here.

C. Problem Formulation

In traditional Ethereum systems, the Gas affects the time and energy consumption of block generation, but has no effect on computational resource allocation. Sensors paying higher Gas desire to get better computational resources. Hence, we define the unsatisfactory degree of U_i allocated M_k as follows,

$$O_i = W_{i,k}\left[r(v_i) - r\left(\frac{f_k}{c_k}\right)\right], \tag{5}$$

where $W_{i,k}$ is the i-th row and k-th column of $\mathbf{W}$. $W_{i,k}$ is a binary variable taking 1 when M_k is assigned to U_i, and 0 otherwise. $r(v_i)$ is the index of the descending order of $\{v_1, ..., v_{N_I}\}$, and $r(f_k/c_k)$ is the index of the descending order of $\{f_k/c_k, ..., f_{N_I}/c_{N_I}\}$. Here, $N_K - N_I$ weaker computational resources are abandoned.

With the consideration of the energy consumption and degrees of satisfaction, the problem of the computation offloading usually focuses on the energy consumption minimization with constraints as follows.

$$\text{P1:} \min_{\mathbf{\Phi}_i, \forall i, \mathbf{W}} \sum_{i=1}^{N_I} \sum_{k=1}^{N_K} W_{i,k} Q_{i,k}, \tag{6}$$

$$\text{s.t. } O_i \le \epsilon, \forall i, \tag{7}$$

$$W_{i,k} = \{0 \text{ or } 1\}, \forall i, k, \tag{8}$$

$$\sum_{i=1}^{N_I} W_{i,k} \le 1, \quad \sum_{k=1}^{N_K} W_{i,k} \le 1, \tag{9}$$

$$\text{Eq. } (1). \tag{10}$$

where Eq. (7) requires that the unsatisfactory degree of U_i should be small than a threshold ϵ, and $\epsilon \in [0, 1, ..., N_I - 1]$ that can be adjusted manually. Eq. (8) is the binary constraint representing allocation factor. Eq. (9) reveals that each sensor can be allocated with only one MEC server, and each MEC server is only assigned to one sensor. Eq. (10) is the passive phase shifter constraint.

It is obvious that $\mathbf{\Phi}_i, \forall i$ and $\mathbf{W}$ are independent variables in optimization, and P1 is non-convex mixed-integer problem. To tackle the problem, we transform P1 into two sub-problem, i.e., phase shift optimization and computational resource allocation, then solve them step-by-step.

III. Computation Offloading Scheme with assistance of IRS and MEC Server

A. Phase Shift Optimization

From Eq. (4), we can find that the energy consumption $Q_{i,k}$ decreases with the increasing ergodic secrecy rate R_i for all sensors. Firstly, we should find the optimal $\mathbf{\Phi}_i$ to maximize R_i, where R_i is given as follows [11],

$$R_i = [\mathbb{E}(C_{m,i}) - \mathbb{E}(C_{w,i})]^+ \tag{11}$$

$$\le \mathbb{E}[(C_{m,i} - C_{w,i})^+)], \tag{12}$$

where

$$C_{m,i} = B \log_2 \left(1 + \frac{\alpha_i^2 P_i}{\sigma_i^2} |l_i + \mathbf{a}_i^{\mathrm{H}} \mathbf{\Phi}_i \mathbf{h}_i|^2\right), \tag{13}$$

$$C_{w,i} = B \log_2 \left(1 + \frac{\alpha_{e,i}^2 P_i}{\sigma_{e,i}^2} |g_i + \mathbf{z}_i^{\mathrm{H}} \mathbf{\Phi}_i \mathbf{h}_i|^2\right), \tag{14}$$

and B is the bandwidth. $\{=\}$ in Eq. (12) holds if and only if the instantaneous secrecy rate $\{C_{m,i} - C_{w,i}\}$ is nonnegative in all channel state. Due to Eve's CSI g_i and $\mathbf{z}$ are unknown, it is hard to determine whether an instantaneous secrecy rate is nonnegative or not, so we use the lower bound of real ergodic secrecy rate as the performance metric for the optimization process. The objective is to find the optimal $\mathbf{\Phi}_i$ to achieve $R_i^* = \max_{\mathbf{\Phi}} R_i$ and get the expression of R_i^* for the following computational resource allocation. However, it is hard to maximize R_i as g_i and $\mathbf{z}$ are unknown, so the objective is transformed to maximize the channel capacity between U_i and the SBS as follows,

$$\text{P2:} \max_{\mathbf{\Phi}} \mathbb{E}(C_{m,i}), \tag{15}$$

$$\text{s.t. Eq. } (1). \tag{16}$$

From the investigation in [12], the optimal $\mathbf{\Phi}_i$ of P2, i.e., $\mathbf{\Phi}_i^*$, can be found as follows,

$$\theta_{i,n}^* = \theta_i - \arg(a_{i,n}^{\mathrm{H}}) - \arg(h_{i,n}), n = 1, ..., N, \tag{17}$$

where $\theta_{i,n}^*$ is the n-th diagonal element in $\mathbf{\Phi}_i^*$, $\theta_i = \arg(l_i)$, $a_{i,n}^{\mathrm{H}}$ is the n-th element of $\mathbf{a}_i^{\mathrm{H}}$, and $h_{i,n}$ is the n-th element of $\mathbf{h}_i$. Here, $\arg(x)$ is the angle of a complex variable x.

Theorem 1 (Expression of optimal ergodic secrecy rate)**.** The expression of optimal ergodic secrecy rate of U_i with $\mathbf{\Phi}_i^*$ can be expressed as

$$R_i^* = [\mathbb{E}(C_{m,i}|\mathbf{\Phi}^*) - \mathbb{E}(C_{w,i}|\mathbf{\Phi}^*)]^+, \tag{18}$$

where

$$\mathbb{E}(C_{m,i}|\mathbf{\Phi}^*) \tag{19}$$

$$= \frac{2^{\mu_1-1/2}}{\ln(2)\Gamma(\mu_1)\sqrt{2\pi}} G_{3,5}^{5,1}\left(\frac{\sigma^2}{4\nu_1^2 P_i \alpha_i^2}\middle| \begin{matrix} 0, \frac{1}{2}, 1 \\ 0, 0, \frac{1}{2}, \frac{\mu_1}{2}, \frac{\mu_1+1}{2} \end{matrix}\right), \tag{20}$$

$$\mu_1 = \frac{(\sqrt{\pi}+2\eta\kappa N)^2}{4+4\eta\kappa^2 N-\pi}, \quad \nu_1 = \frac{4+4\eta\kappa^2-\pi}{2(\sqrt{\pi}+2\eta\kappa N)}, \tag{21}$$

$\eta = \pi^2/(16-\pi^2)$, and $\kappa = (4-\pi^2/4)\pi$.

$$\mathbb{E}(C_{w,i}|\mathbf{\Phi}^*) = \frac{1}{\ln(2)\Gamma(\mu_2)} G_{2,3}^{3,1}\left(\frac{\sigma_{e,i}^2}{\nu_2 P_i \alpha_{e,i}^2}\middle| \begin{matrix} 0, 1 \\ 0, 0, \mu \end{matrix}\right), \tag{22}$$

where

$$\mu_2 = \frac{(1+N)^2}{(1+N)^2+2N}, \quad \nu_2 = 1+N+\frac{2N}{1+N}. \tag{23}$$

Proof. The similar proof of Eqs. (19) and (22) can be found in [13, Eq. (21)] and [13, Eq. (20)], respectively. Substituting Eqs. (19) and (22) into Eq. (13), we can obtain the expression of optimal ergodic secrecy rate. ■

B. Gas-Oriented Computational Resource Allocation

The optimal computational resource allocation is found by grouping and matching algorithms.

1) Grouping process: In order to meet the satisfactory degree of each sensor, i.e., constraint (7), the sensors are sort as $\{U_{1'}, U_{2'}, ..., U_{N_I'}\}$ where their Gas obey $V_{1'} \geq V_{2'} \geq ... \geq V_{N_I'}$, and are grouped into $T = \lceil \frac{N_I}{\epsilon+1} \rceil$ groups. Each group includes $\epsilon+1$ members as follows,

$$\overbrace{\{U_{1'}, U_{2'}, ..., U_{(\epsilon+1)'}\}}^{\text{first sensor group}}, \quad \overbrace{\{U_{(\epsilon+2)'}, U_{(\epsilon+3)'}, ..., U_{(2\epsilon+2)'}\}}^{\text{second sensor group}},$$
$$..., \overbrace{\{U_{[(T-1)\epsilon+T]'}, U_{[(T-1)\epsilon+T+1]'}, ..., U_{N_I'}\}}^{\text{last sensor group}}. \tag{24}$$

Specially, the last sensor group has $\{N_I - (T-1)(\epsilon+1)\}$ members. Similarly, the MEC servers are sort as $\{M_{1''}, M_{2''}, ..., M_{N_I''}\}$ where their computational power obey $f_{1''}/c_{1''} \geq f_{2''}/c_{2''} \geq ... \geq f_{N_I''}/c_{N_I''}$ by dropping $N_K - N_I$ weaker MEC servers, and are grouped into T groups. Each group includes $\epsilon+1$ members as follows,

$$\overbrace{\{M_{1''}, U_{2''}, ..., M_{(\epsilon+1)''}\}}^{\text{first MEC group}}, \quad \overbrace{\{M_{(\epsilon+2)''}, M_{(\epsilon+3)''}, ..., M_{(2\epsilon+2)''}\}}^{\text{second MEC group}},$$
$$..., \overbrace{\{M_{[(T-1)\epsilon+T]''}, M_{[(T-1)\epsilon+T+1]''}, ..., M_{N_I''}\}}^{\text{last MEC group}}. \tag{25}$$

The last MEC group has $\{N_I - (T-1)(\epsilon+1)\}$ members. The MEC server in the t-th MEC group is only allocated to the t-th sensor group, and the sensor in the t-th sensor group can only uses computational resources in the t-th MEC group. From Eq. (5), we can find that $r(v_i) - r(f_k/c_k) \leq \epsilon$ for any sensor and MEC server pair, so the constraint (7) is satisfied.

2) Matching process: Without loss of generality, we define $\mathcal{S}_t = \{[(t-1)\epsilon+t]', ..., t(\epsilon+1)'\}$ and $\mathcal{M}_t = \{[(t-1)\epsilon+t]'', ..., t(\epsilon+1)''\}$ as the indices of the members in the t-th sensor group and the t-th MEC group. Then, we use Theorem 1 to calculate optimal ergodic secrecy rates of all sensors, i.e., $R_i^*, \forall i \in \mathcal{S}_t$. With the parameters $\{\eta_k, c_k, f_k, D_i, P_i, R_i^*\}, \forall i \in \mathcal{S}_t, \forall k \in \mathcal{M}_t$, we can calculate $Q_{i,k}$ via Eq. (4) for each given sensor and MEC server pair, and generate a matrix $\mathbf{Q}$ to record $Q_{i,k}, \forall i \in \mathcal{S}_t, \forall k \in \mathcal{M}_t$. The allocation problem in the t-th sensor group and the t-th MEC group can be equivalently transformed to a 2-dimensional matching problem as

$$\text{P3: } \min_{\mathbf{W}_t} \sum_{i=(t-1)\epsilon+t}^{\epsilon+1} \sum_{k=(t-1)\epsilon+t}^{\epsilon+1} W_{t,i,k} Q_{i,k}, \tag{26}$$

$$\text{s.t. } W_{t,i,k} = \{0 \text{ or } 1\}, \forall i, k, \tag{27}$$

$$\sum_{i=(t-1)\epsilon+t}^{\epsilon+1} W_{t,i,k} \leq 1, \quad \sum_{k=(t-1)\epsilon+t}^{\epsilon+1} W_{t,i,k} \leq 1, \tag{28}$$

where $W_{t,i,k}$ is the i-th row and k-th column of $\mathbf{W}_t$. $W_{t,i,k}$ is a binary variable taking 1 when M_k in t-th MEC group is assigned to U_i in the t-th sensor group, and 0 otherwise. Eq. (28) reveals that each sensor can be allocated with only one MEC server, and each MEC server is only assigned to one sensor. P3 is convex and the optimal $\mathbf{W}_t$ can be solved by the Kuhn-Munkres (KM) algorithm [14]. Even if the number of dimensional in the last group is different from the formers, computational resource allocation in all T sensor and MEC groups, including the last group, can be optimized via the KM algorithm.

C. Computational Complexity Analysis

In the phase optimization process, Since Eq. (17) requires $2N$ iterations, the computational complexity to get $\mathbf{\Phi}_i^*, \forall i$ is $O(2NN_I)$. The computational resource allocation requires two bubble sort algorithms to get $\{U_{1'}, U_{2'}, ..., U_{N_I'}\}$ and $\{M_{1''}, M_{2''}, ..., M_{N_I''}\}$, each of which needs N_I^2 iterations. The KM algorithm needs $(\epsilon+1)^4$ iterations in each group pair [14]. In total, the computational complexity of the offloading process is $O[2NN_I + 2N_I^2 + T(\epsilon+1)^4]$.

IV. Simulations

The global simulation parameters are described as follows. The path loss parameter α_i is calculated by $\alpha_i = \frac{c}{2\pi f_c d_i}$, where c is the speed of light, f_c is work spectrum that is set to 2.4 GHz, d_i is the distance between the SBS and U_i is set to be uniform distribution over [30 m, 50 m]. The AWGN floor parameters σ_i^2 and $\sigma_{e,i}^2$ are -53 dBm [15]. The transmission power $P_i, \forall i$ is 10 dBm. The computation energy efficiency coefficient $\eta_k, \forall k$ is set to be 10^{-27}. The CCN per bit processing $c_k, \forall k$ is set to be 10 CCN/bit. Note that all simulation results are average values from 10^5 independent runs.

Here, we examine Theorem 1 in terms of the number of IRS elements in Fig. 2. These figures show the good

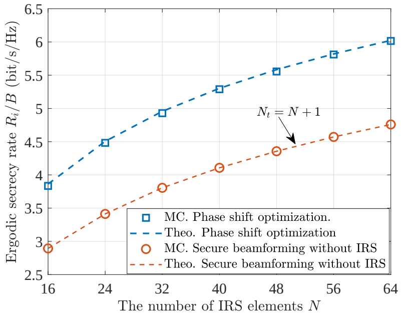

Fig. 2: Optimal ergodic secrecy rate of U_i in terms of the number of IRS elements.

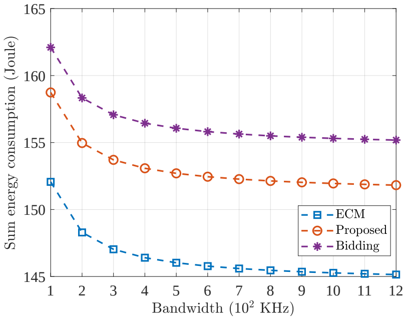

Fig. 3: Sum energy consumption of 40 sensors in terms of the length of bandwidth.

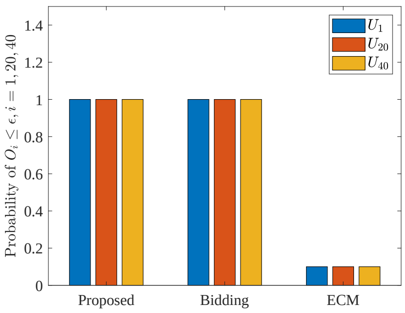

Fig. 4: The probability of satisfaction of U_1, U_{20}, and U_{40}.

agreements between theoretical results (Theo.) of Eq. (18) and Monte Carlo (MC.) simulation results of Eq. (13) from 10^5 independent runs. From this figure, we can find that the optimal ergodic secrecy rate increases with the increasing number of IRS elements. Also, a comparison is taken between IRS-assisted PLS and the secure beamforming scheme that uses $N_t = N + 1$ antennas [11]. From the comparison simulations, we find that the IRS-assisted PLS outperforms the secure beamforming scheme because channel gain by IRS is larger than that of the beamforming scheme [13].

Fig. 3 shows the bandwidth effect on the sum energy consumption of 40 sensors, where $\epsilon = 9$. f_k, D_i, and V_i are uniform distributions over [40 GHz, 80 GHz], [610 KB 1.8 MB], and $[1.5 \times 10^6, 2 \times 10^6]$. It is demonstrated that the sum energy consumption decreases with the increasing bandwidth, because data transmission time is reduced with more bandwidth. Also, the proposed scheme outperforms the bidding scheme (the highest bidder obtains), but has worse performance than energy consumption minimization (ECM) schemes [5], [6]. Fig. 4 with the simulation parameters of Fig. 3 is used to check whether sensors are satisfied. We can find the probabilities of the satisfaction of the proposed scheme and bidding scheme is equal to one, meaning that sensors are satisfied. However, the provided Gas has no relationship with computational resource allocation in the ECM schemes, so the probability of $O_i \leq \epsilon$ is equal to $1/T$, where $T = N_I/(\epsilon + 1) = 10$ in this simulation.

V. Conclusions

In this article, we establish a blockchain-empowered computation offloading system in an IoT network, where the data is protected by IRS-assisted PLS methods. Especially, we design a Gas-oriented grouping algorithm where the group with higher Gas is prioritized with better computational resources. The simulations show that the proposed computational resource allocation reduces the energy consumption while guaranteeing that the node paying higher Gas has more opportunities to get a stronger computational resource. As one of our future works, we will integrate multiple antenna technologies into this system as it is a promising method to improve security performance.

References

[1] J. Wang, X. Ling, Y. Le, Y. Huang, and X. You, “Blockchain enabled wireless communications: A new paradigm towards 6G,” *National Science Review*, vol. nwab069, Apr. 2021.

[2] Y. He, Y. Wang, C. Qiu, Q. Lin, J. Li, and Z. Ming, “Blockchain-based edge computing resource allocation in IoT: A deep reinforcement learning approach,” *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2226–2237, Jan. 2021.

[3] C. Qiu, X. Wang, H. Yao, J. Du, F. R. Yu, and S. Guo, “Networking integrated cloud–edge–end in IoT: A blockchain-assisted collective Q-learning approach,” *IEEE Internet Things J.*, vol. 8, no. 16, pp. 12 694–12 704, Aug. 2021.

[4] Y. Wang, Z. Su, N. Zhang, J. Chen, X. Sun, Z. Ye, and Z. Zhou, “SPDS: A secure and auditable private data sharing scheme for smart grid based on blockchain,” *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7688–7699, Nov. 2021.

[5] Y. Wang, M. Sheng, X. Wang, L. Wang, and J. Li, “Mobile-edge computing: Partial computation offloading using dynamic voltage scaling,” *IEEE Trans. Commun.*, vol. 64, no. 10, pp. 4268–4282, Oct. 2016.

[6] J. Feng, F. R. Yu, Q. Pei, J. Du, and L. Zhu, “Joint optimization of radio and computational resources allocation in blockchain-enabled mobile edge computing systems,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 6, pp. 4321–4334, Jun. 2020.

[7] Y. Liu, W. Wang, H.-H. Chen, F. Lyu, L. Wang, W. Meng, and X. Shen, “Physical layer security assisted computation offloading in intelligently connected vehicle networks,” *IEEE Trans. Wireless Commun.*, vol. 20, no. 6, pp. 3555–3570, Jun. 2021.

[8] J. Du, L. Zhao, J. Feng, and X. Chu, “Computation offloading and resource allocation in mixed fog/cloud computing systems with min-max fairness guarantee,” *IEEE Trans. Commun.*, vol. 66, no. 4, pp. 1594–1608, Apr. 2018.

[9] S. Xiong, Q. Ni, L. Wang, and Q. Wang, “SEM-ACSIT: Secure and efficient multiauthority access control for IoT cloud storage,” *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2914–2927, Jan. 2020.

[10] J. Li, Z. Su, D. Guo, K.-K. R. Choo, and Y. Ji, “PSL-MAAKA: Provably secure and lightweight mutual authentication and key agreement protocol for fully public channels in internet of medical things,” *IEEE Internet Things J.*, vol. 8, no. 17, pp. 13 183–13 195, Sep. 2021.

[11] Y. Liu, H.-H. Chen, L. Wang, and W. Meng, “Artificial noisy MIMO systems under correlated scattering Rayleigh fading — A physical layer security approach,” *IEEE Syst. J.*, vol. 14, no. 2, pp. 2121–2132, Jun. 2020.

[12] Q. Wu and R. Zhang, “Intelligent reflecting surface enhanced wireless network via joint active and passive beamforming,” *IEEE Trans. Wireless Commun.*, vol. 18, no. 11, pp. 5394–5409, Nov. 2019.

[13] T. Van Chien, L. T. Tu, S. Chatzinotas, and B. Ottersten, “Coverage probability and ergodic capacity of intelligent reflecting surface-enhanced communication systems,” *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 69–73, Jan. 2021.

[14] R. Duan and H.-H. Su, “A scaling algorithm for maximum weight matching in bipartite graphs,” Jan. 2012, pp. 1413–1424.

[15] T. Dinc, A. Chakrabarti, and H. Krishnaswamy, “A 60 GHz CMOS full-duplex transceiver and link with polarization-based antenna and RF cancellation,” *IEEE J. Solid-State Circuits*, vol. 51, no. 5, pp. 1125–1140, May 2016.