Weighted RAFT: An Improved Blockchain Consensus Mechanism for Internet of Things Application

Xiaojun Xu*, Lu Hou Member, IEEE, Yankai Li, Yunxin Geng
*Intelligent Computing and Communications Lab,
Key Lab of Universal Wireless Communications, Ministry of Education,
Beijing University of Posts and Telecommunications, Beijing, China
xuric@bupt.edu.cn

2021 7th International Conference on Computer and Communications (ICCC) | 978-1-6654-0950-6/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICCC54389.2021.9674683

***Abstract*—The integration of blockchain technology and RAFT consensus algorithm could address many of the IoT application security and privacy issues. However, each node in RAFT consensus has equivalent probability of being elected as a leader, which takes no consideration on the communication and computing status of the node. Therefore, in this paper, we propose a weighted RAFT consensus algorithm for IoT applications, which allows IoT gateway with better capacity to have a higher possibility of being elected as the leader compared to the normal RAFT mechanism. Thus, the latency of uploading IoT data on blockchain can be reduced a lot. Simulation results show that the weighted RAFT can reduce the system forwarding latency by 24% at most.**

Keywords—IoT; Blockchain; weighted RAFT; leader election

I. INTRODUCTION

The fifth-generation (5G) brings a huge advancements and evolutions for wireless communications and networking, which supports the development of the Internet of Things (IoT) applications. It is expected that there will be large-scale IoT device proliferation to satisfy diverse requirements of IoT. By 2021, the total number of connected devices has reached 28 billion [1]. The number of IoT connections will reach 1 trillion in 2035, with an annual economic impact of $ 2.7-6.2 trillion [2]. The development of IoT will provide effective support for smart homes, industrial control, public safety, environmental protection, autonomous driving, telemedicine and other applications [3], [4].

One of the main problems restricting IoT applications is data privacy and security. Traditional IoT systems usually apply centralized architectures. The system can be out of services when the center server crashes or being attacked. Meanwhile, the IoT data needs to be uploaded to the traditional database, where the administrator can access the data without the permission of data owner. As a decentralized ledger, blockchain technology can well address data privacy and security issues in IoT. Blockchain does not rely on any third party and can store, verify and transfer data through its own decentralized nodes safely [5], [6].

The consensus mechanism is the key to ensure data consistency and security of blockchain system. It also has significant influence on the performance of IoT system. Proof of Work (PoW) or Proof of Stake (PoS) mechanisms are generally applied in public blockchain for consensus. Practical Byzantine Fault Tolerance (PBFT) or non-Byzantine Fault Tolerance such as RAFT and PoET are commonly used in consortium blockchain for consensus. In IoT system, terminals usually have low capabilities on computing, communication and energy. Thus they cannot undertake heavy consensus tasks. RAFT algorithm is succint and requires little computation and communication ability, which is suitable to be applied in IoT devices. In RAFT algorithm, all nodes have the same probability to be elected as the leader. However, due to the various and changing conditions of different IoT devices, the performance cannot be fully exploited. It is necessary to design a new leader election mechanism for RAFT to improve the efficiency of IoT system with blockchain.

Therefore, this paper proposes a consensus method called weighted RAFT (WRAFT) algorithm. In WRAFT, the leader will collect the number of data packages that are forwarded by followers and the wireless channel states between all nodes. The information is collected via heartbeat message. The leader then evaluates the capability of each node and computes a weight that can reflect the ability. Nodes with higher weight values are more likely to get shorter timeouts during the leader election phase. Therefore, WRAFT can provide high possibility for nodes with better capabilities to serve as the leader. Then, the performance of the whole IoT system can be enhanced a lot.

The rest of the paper is organized as follows. Section II discusses related works. The system model is formulated in Section III. Section IV discusses the details of proposed leader election mechanism. The performance test is shown in Section V with results analysis. Section VI concludes the paper.

II. RELATED WORKS

A blockchain system is a decentralized system that relies on a consensus algorithm to ensure consistency in the state of certain data among several nodes. As one of the most important components of a blockchain system, the efficiency of consensus algorithm influences a lot on the performance of blockchain system, especially for resource-constrained IoT devices. For public blockchain, which allows anyone to

participate in to create and verify blocks, the most adopted consensus mechanism is called Proof of Work (PoW). PoW ensures system security and can resist security threats such as double spending attack, selfish mining attack and eclipse attack with less than 51% of mining capacity [7], [8]. However, PoW is inefficient and wastes a lot of energy. Therefore, Proof of Stake (PoS) consensus, as well as several kinds of variants, has been proposed and applied in Ethereum [9]. The stake in PoS acts as a guarantee that the stakeholder can behave strictly as the protocol rules.

In contrast to the public blockchain, consortium blockchain has a restrictive concept that only authorized and trusted entities can participate in the activities within the blockchain. One of the most applicable consensus mechanism used in the consortium blockchain is Byzantine Fault Tolerance (BFT) [10] and the practical version, i.e., Practical BFT [11]. PBFT deals with nodes that misbehave due to some bugs or being compromised by an attacker. The maximum number of Byzantine nodes that can be tolerable by PBFT is $f < [n/3]$, where f is the number of Byzantine nodes and n denotes the total nodes in the network. To improve the efficiency of PBFT, several BFT based consensus are developed. For example, [12] proposed SBFT consensus mechanism, and [13] applies SBFT consensus mechanism to blockchain. The SBFT consensus mechanism uses collector technology and collector communication mode, which significantly reduces the communication volume. However, the BFT still needs a lot of message exchanges between primary node and follower node to avoid the Byzantine node comproimising the system.

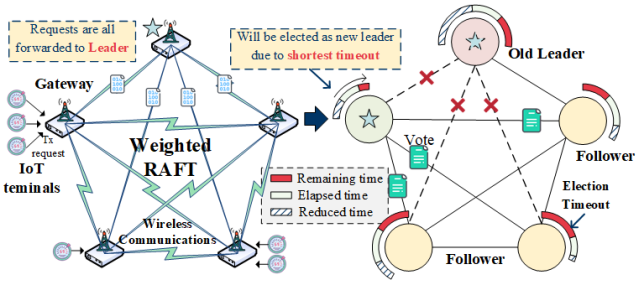

Fig. 1. System model

In IoT applications, each node needs to be authenticated before entering the network. Thus, it can be assumed that nodes in the IoT system are trustworthy. Therefore, RAFT consensus algorithm can be deployed to improve the efficiency for consensus [14, 15]. The RAFT requires a leader election process, and the consensus is finalized totally by the leader. Then, the need for message exchanges is reduced a lot, compared to PBFT. Recently, there are some other researches focusing on improving the performance of RAFT. *Rihong Wang et al.* [16] proposed KRAFT, which is a RAFT-like consensus algorithm based on the Kademlia protocol [17]. It optimized the leader election and consensus process of the RAFT algorithm through the established K-Bucket node relationship and also improved leader election speed and throughput. *Hao Xu et al.* [18] proposed a RAFT-based wireless blockchain network, which can improve the security performance of wireless blockchain networks in the presence of malicious jamming. *Zizhong Wang et al.* [19] proposed the CRAFT algorithm by using erasure coding to save storage and network costs, while keeping the same liveness as RAFT. To the best of our knowledge, none of the researches focuses on improving the performance of RAFT-based IoT blockchain network by taking the computing ability and the wireless communication environment into account during the leader election phase of RAFT.

III. System Model

A. Scenario Description

The system scenario is shown in Fig. 1. We assume the numbers of IoT end-devices and gateways are denoted by M and N, respectively. Each gateway covers a certain number of IoT end-devices, collecting the data and forwarding them to edge server or center server. Assume that the number of arriving packets follows Poisson distribution with intensity λ, i.e.,

$$p(i) = \frac{\lambda^i}{i!} e^{-\lambda}, \tag{1}$$

To ensure the security of the IoT system, a blockchain network is considered to be deployed on gateways.

B. Communication Model

IoT end-devices collect and report data at fixed intervals to gateways by wireless communication. Assume the system running time is divided into multiple slots. The legal generation and uploading of blocks in the previous slot is regarded as the beginning of the next slot. Meanwhile, assume that each IoT end-device in the scenario only collects data of a single application type and has the same data transmission power. Each end-device reports data at the beginning of the slot simultaneously. The data transmission rate between the gateway m and the gateway n is calculated according to Shannon equation,

$$r_{m,n} = \frac{B}{I} \log_2 \left(1 + \gamma_{m,n}\right), \tag{2}$$

where B is the available bandwidth of the system, which is evenly allocated to IoT gateways in the system for data transmission. $\gamma_{m,n}$ is the signal-to-noise ratio (SNR) of data transmission between the gateway m and the gateway n,

$$\gamma_{m,n} = P_n + G_m + G_n - \mathrm{PL} - X(\mathrm{dB}), \tag{3}$$

where P_n is transmission power, G_m represents transmitter antenna gain, G_n represents receiver antenna gain, $X \sim N\left(0, \sigma^2\right)$ stands for the additive white gaussian noise, and PL adopts empirical model is given by,

$$\mathrm{PL} = 32.44 + 20 \lg d_{m,n} + 20 \lg f(\mathrm{dB}), \tag{4}$$

where $d_{m,n}$ represents the distance between the gateway *m* and the gateway *n*, *f* represents transmission frequency.

C. RAFT Algorithm

1) Heartbeat mechanism: In the RAFT algorithm, each node changes its node status between leader, follower, and candidate. The leader demonstrates its liveness through the heartbeat mechanism. When the follower fails to receive the heartbeat data packet within a specified period, it will convert to a candidate and trigger the leader election process. Meanwhile, there is a difference in leader election timeout between different followers and the specific timeout for followers are randomly chosen. The follower with a shorter timeout can be converted to a candidate faster than those with longer timeouts. Therefore, heartbeat mechanism of the RAFT algorithm is a random algorithm, which aims to make it possible for all followers in the network to be elected as the leader in the long-term operation to ensure crash tolarence.

2) Leader selection mechanism: Leader selection is triggered by missing of the heartbeat message. In the leader selection process, all candidates broadcast voting requests in the blockchain network to obtain a majority votes to become the new leader. The followers who failed to convert to the candidate are the node with voting rights in the blockchain network. The follower will elect for the first candidate from which it receives the voting request. After a voting process, if no candidate obtains majority votes, leader selection will be restarted again until a new leader is finalized. The candidate that wins the leader selection first changes its node status and sends the heartbeat message to the rest of nodes in the blockchain network to demonstrate its leadership and synchronize blocks.

3) Block consensus: The IoT data is packaged into new blocks only by the leader. The leader collects data in the form of transactions to generate blocks at fixed intervals. Then the block is sent to other gateways in the network for endorsement. If the leader receives more than $N/2$ confirmation responses, it indicates that the quorum is reached and new block can be uploaded to the blockchain. If a gateway fails to receive the new block broadcast by the leader in the blockchain network, the gateway will not be able to update the block synchronously. Until the gateway receives a new block, leader will check the ledger consistency between the gateway and the leader. The gateway's ledger is compared with the leader's ledger to update itself autonomously.

IV. Design of Weighted RAFT Algorithm

A. Design of Heartbeat Mechanism

To improve the efficiency of the IoT blockchain system, it is necessary to design a consensus algorithm that can fit the characteristics of the IoT system. The proposed WRAFT uses heartbeat message to collect status of followers and calculate a weight for each of them to determine the timeout value in leader election phase. The number of data forwarded by each gateway is represented by L_n, which is expressed as follows,

$$L_n = \sum_{m \in D_n} j_m, \tag{5}$$

where j_m is the number of data reported by end-device *m*, and D_n is a collection of IoT end-devices that report data to gateway *n*. WRAFT algorithm takes the number of data forwarded by each gateway and the wireless communication environment as the evaluation index to adjust the timeout of each gateway and make the optimal leader selection. The wireless communication environment of each gateway is determined by the SNR between a gateway and others during data forwarding. The specific communication environment calculation method is given as follows,

$$\overline{\mathrm{SNR}}_n = \frac{1}{K-1} \sum_{k=1,k\neq n}^{K} \gamma_{n,k}. \tag{6}$$

In order to evaluate the gateway comprehensively, this paper considers L_n and $\overline{\mathrm{SNR}}_n$ to design the following evaluation formula to calculate the weight value of the gateway *n*,

$$w_n = \alpha_1 \frac{L_n}{L_{max}} + \alpha_2 \frac{\overline{\mathrm{SNR}}_n}{\overline{\mathrm{SNR}}_{\max}}. \tag{7}$$

where α_1 and α_2 are the coefficients of L_n and $\overline{\mathrm{SNR}}_n$, respectively.

According to the weight value of gateways, each gateway will start a clock with its specific timeout. Every time the leader broadcasts a heartbeat packet in the blockchain network, it has to perform a timeout calculation. The relation of w_n and the timeout t_n is given as follows,

$$t_n \sim U\left(A, B + \beta w_n \tau\right), \tag{8}$$

where *A* and *B* decides the minimum interval of timeout, and τ, β are constants. When the leader fails, it can make the best leader selection according to the real-time updated by

communication environment.

B. Latency Analysis

To evaluate the influence of the leader election in WRAFT on system performance, this paper uses data forwarding latency as a metric to evaluate the influence of the leader election on system performance.

In the RAFT algorithm, transactions need to be forwarded to the leader by followers, because all blocks are generated only by the leader. The forwarding latency of all follower is defined as follow,

$$\sum_{k=1,k\neq l}^{K} \frac{D}{r_{k,l}}, \tag{9}$$

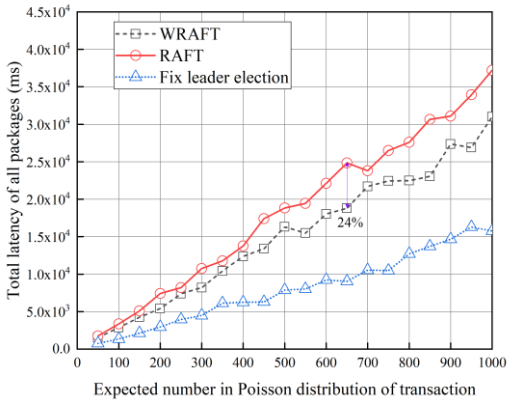

Fig. 2. Illustration on total latency of all packages under Poisson arrival.

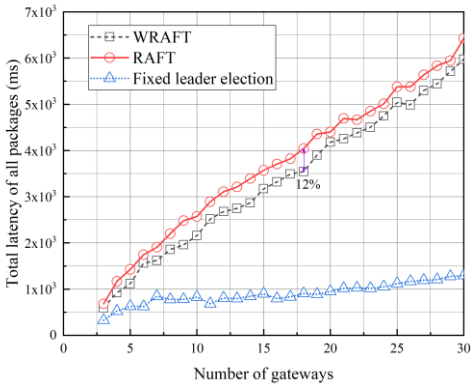

Fig. 3. Illustration on total latency of all packages under different number of gateways number

TABLE I. PARAMETER CONFIGURATION

Parameter	Value	Parameter	Value
P_n	20 dBm	α_1	0.3
G_m	10 dBi	α_2	0.7
G_n	10 dBi	β	5
f	2 GHz	σ	10
λ	25 ms	λ	50

where D is the total of transactions data size. Meanwhile, to confirm the weight value of followers, the information of L_n and $\overline{\mathrm{SNR}}_n$ need to be transport to leader, which will cost a bit more latency during the leader election. The election latency is defined as follow,

$$t_{\text{election}} = \sum_{k=1,k\neq l}^{K} \frac{V+H}{r_{k,l}}, \tag{10}$$

where k stands for the index of follower and l represents the leader, and V, H represent the vote package and extra information size of T_n and $\overline{\mathrm{SNR}}_n$, respectively.

V. PERFORMANCE EVALUATION AND ANALYSIS

A. Environment Setup

A simulation is conducted to evaluate the performance of WRAFT. The number of gateways ranges from 3 to 30 and the expected number of the Poisson distribution of request packages arrival ranges from 100 to 1,000. Two baselines are introduced, i.e., the normal RAFT and the fixed leader election machanism. RAFT gives equal probability for all nodes to be elected as the leader, while fixed leader election mechanism chooses the leader with highest weights, i.e.,

$$l = \arg\max_{n\in[0,N]} w_n. \tag{11}$$

The limit election timeout in this simulation of A and B is set to be 150ms and 200ms. The main parameters are listed in Table. I.

B. Evaluation Results and Analysis

As shown in Fig. 2, when the number of gateways is 5, the total latency of the WRAFT is reduced 24% comparing the original RAFT when the expected number in the Poisson distribution of request packages arrival changing.

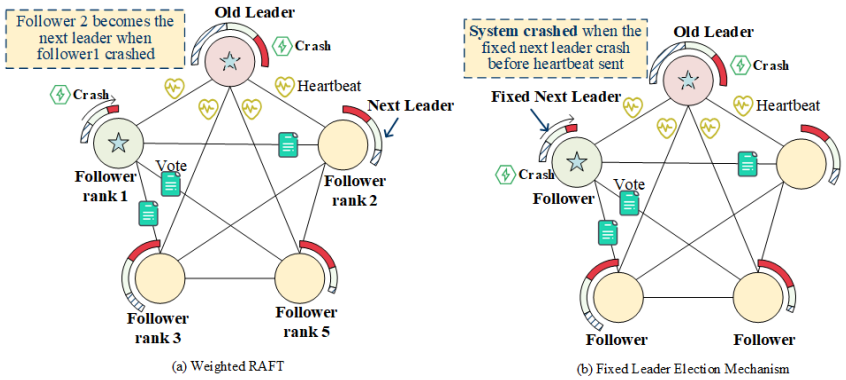

Fig. 4. Illustration on the analysis of system robustness between WRAFT and Fixed Leader Election

When λ is 50, the total latency of the WRAFT is reduced by 12% comparing the original RAFT when the number of gateways changing as shown in Fig. 3. Meanwhile, the fixed leader election mechanism reaches the lowest latency of the three. However, the system robustness can be demonstrated by Fig. 4. Through the WRAFT, followers get a timeout according to the w_n to be elected as a leader. Instead, the fixed leader election mechanism fixed the next leader according to the w_n to minimize the system latency which lost the randomness. When leader and the first ranking follower crash, the WRAFT will possibly select the second ranking follower as the next leader, while the fixed leader election mechanism will halt because no leader will be elected if the heartbeat message is not sent before the previous leader crashed.

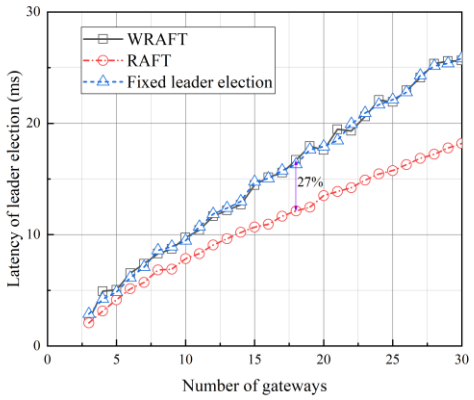

Fig. 5. Latency of leader election.

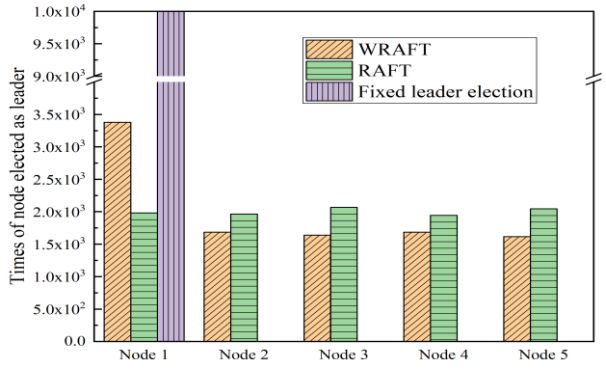

Fig. 6. Times of Node Elected as Leader

We evaluate the latency of leader election when RAFT nodes changing from 3 to 30 in Fig. 5. To calculate the weight value, the followers of WRAFT need to upload additional information of communication state. So that the WRAFT costs nearly more 27% latency than the original RAFT, while the absolute number is only 4ms. Similarly, the fixed leader election mechanism performs equal latency to the WRAFT.

As shown in Fig. 6, we simulated the process of leader election 10,000 times of a 5 nodes system and calculated the distribution of leader election. The result shows that in the normal RAFT, the times of each node elected as the leader is nearly equal. But in the WRAFT, Node 1 with better performance is more likely to be elected as the leader, while the other nodes also have chance to be elected as the leader, which
ensures the availability of IoT system. However, the fixed leader election mechanism always selects Node 1 as the leader, which is more easily to crash.

VI. Conclusion

In this paper, we proposed a weighted RAFT algorithm that can improve the efficiency of normal RAFT in IoT applications with equal ability of crash tolerance. WRAFT elects the leader with consideration to the wireless communication environment and the computing tasks. Therefore, follower with better performance has a higher probability of being elected as the leader, leading to an improvement on the latency of the whole system. Simulation results show that WRAFT can reduce at most by 24\% in data packages forwarding and costs only 4ms more in leader election.

Acknowledgment

This work was supported by the National Natural Science Foundation of China (No. 62001052).

References

[1] E. Sisinni, A. Saifullah, S. Han, U. Jennehag and M. Gidlund, "Industrial Internet of Things: Challenges, Opportunities, and Directions," in IEEE Transactions on Industrial Informatics, vol. 14, no. 11, pp. 4724-4734, Nov. 2018, doi: 10.1109/TII.2018.2852491.

[2] Salam A. Internet of things for sustainable community development: introduction and overview[M]//Internet of Things for Sustainable Community Development. Springer, Cham, 2020: 1-31.

[3] Novo O. Blockchain meets IoT: An architecture for scalable access management in IoT[J]. IEEE Internet of Things Journal, 2018, 5(2): 1184-1195.

[4] Gupta A K, Johari R. IOT based electrical device surveillance and control system[C]//2019 4th international conference on internet of things: Smart innovation and usages (IoT-SIU). IEEE, 2019: 1-5.

[5] Dai H N, Zheng Z, Zhang Y. Blockchain for Internet of Things: A survey[J]. IEEE Internet of Things Journal, 2019, 6(5): 8076-8094.

[6] Chen L, Xu L, Shah N, et al. Unraveling blockchain based crypto-currency system supporting oblivious transactions: a formalized approach[C]//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. 2017: 23-28.

[7] King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake[J]. self-published paper, August, 2012, 19(1).

[8] Feng Q, He D, Zeadally S, et al. A survey on privacy protection in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126: 45-58.

[9] Lamport L, Shostak R, Pease M. The Byzantine generals problem[M]//Concurrency: the Works of Leslie Lamport. 2019: 203-226.

[10] Castro M, Liskov B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems (TOCS), 2002, 20(4): 398-461.

[11] Kotla R, Alvisi L, Dahlin M, et al. Zyzzyva: speculative byzantine fault tolerance[C]//Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles. 2007: 45-58.

[12] Gueta G G, Abraham I, Grossman S, et al. Sbft: a scalable and decentralized trust infrastructure[C]//2019 49th Annual IEEE/IFIP international conference on dependable systems and networks (DSN). IEEE, 2019: 568-580.

[13] Ongaro D, Ousterhout J. In search of an understandable consensus algorithm[C]//2014 {USENIX} Annual Technical Conference ({USENIX}{ATC} 14). 2014: 305-319.

[14] Hou L, Xu X, Zheng K, et al. An Intelligent Transaction Migration Scheme for RAFT-based Private Blockchain in Internet of Things Applications[J]. IEEE Communications Letters, 2021

[15] Wang R, Zhang L, Xu Q, et al. K-Bucket based Raft-like consensus algorithm for permissioned blockchain[C]//2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2019: 996-999.

[16] Maymounkov P, Mazieres D. Kademlia: A peer-to-peer information system based on the xor metric[C]//International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002: 53-65.

[17] Xu H, Zhang L, Liu Y, et al. RAFT based wireless blockchain networks in the presence of malicious jamming[J]. IEEE Wireless Communications Letters, 2020, 9(6): 817-821.

[18] Hou L, Zheng K, Liu Z, et al. Design and prototype implementation of a blockchain-enabled LoRa system with edge computing[J]. IEEE Internet of Things Journal, 2020, 8(4): 2419-2430.

[19] Wang Z, Li T, Wang H, et al. Craft: An erasure-coding-supported version of raft for reducing storage cost and network cost[C]//18th {USENIX} Conference on File and Storage Technologies ({FAST} 20). 2020: 297-308.