A Study on Lightweight Sensing Data Verification Scheme for WICN with Blockchain

Shintaro Mori
Department of Electronics Engineering and Computer Science
Fukuoka University
8-19-1 Nanakuma, Jonan-ku, Fukuoka 814-0180, Japan
E-mail: smori@fukuoka-u.ac.jp

***Abstract*—We develop an energy-efficient and reliable wireless information-centric network-based ecosystem for smart-city applications. The proposed scheme utilizes a blockchain-based ledger. Since the conventional mining-based verification method is unsuitable for resource-restricted wireless nodes due to problems with exhaustive computer calculations, our scheme adopts the proof-of-elapsed time consensus method. In this work, we demonstrate the efficiency and feasibility of our scheme through computer simulations.**

Keywords—Wireless information-centric networking; Blockchain; Lightweight data verification scheme

I. INTRODUCTION

Future Wireless Sensor Network (WSN) technologies will provide essential functionalities for smart cities. Sensing data have distinctive features compared to traditional Internet data: namely, they are usually short-lived and require validation. This type of data is costly to collect, store, and deliver due to overwhelming network redundancy. Information-Centric Networking (ICN) [1] is a promising technology poised to replace the conventional Internet architecture in the near future. ICN names each piece of data so that they can identify each other, and the ICN nodes provide an in-network caching for further effective responses. Moreover, the features of ICN can boost location-free data access, i.e., the combination of ICN and a wireless network is suitable, which yields information-centric wireless sensor networks [2] or Wireless ICN (WICN). At the same time, since sensing data have a signature, their originality and integrity can be verified. End-to-end nodes are assured in the current ICN systems, so the proposed scheme relaxes this limitation by using Blockchain (BC). The advantage of BC is that it can provide a distributed, traceable, and immutable ledger without centralized and trusted nodes. However, the data verification process must be performed iteratively for computer calculations, similar to the proof-of-works (PoWs) consensus method. This heavy burden is too much accepted for resource-constrained WICN nodes. The proof-of-stake does not require mining task but is not suitable in an equal peer relationship, resulting in a bias. In light of this background, the proposed scheme utilizes a lightweight consensus method.

The remainder of this paper is organized as follows. Section II describes the proposed scheme. Section III presents numerical results. Finally, Section IV summarizes our findings and concludes the paper.

II. PROPOSED SCHEME

In the proposed scheme, the ICWSN is composed of a group of Sensor Nodes (SNs) and Relay Nodes (RNs), both of which are distributed across the local smart-city area. The proposed scheme overlays the BC on the WICN, and the role of the BC nodes is assigned to the RNs.

As a lightweight verification technique, we utilize the Proof-of-Elapsed-Time (PoET) consensus method. In PoETs, each BC node has a timer, and the first node for which a specified waiting time has elapsed is considered as a winner. Each BC node is classified into one coordinator and several validators, with the coordinator providing a random waiting time to the validators. In contrast to the original PoET method, the proposed scheme rotates the role of the coordinator among the BC nodes. This modification provides fairness and eliminates a single point of failure in the WICN with BC. We assume that the winner node of the k th block (k = 0 means the genesis block) is the n-th BC node (n = 1, 2, ⋯, N), and the next competition for the $(k+1)$-th block is conducted among the n th node as a coordinator and $(N-1)$ nodes as validators. For the initial process, the validator broadcasts the signed request message, and the coordinator replies with the latest block index and a random waiting time after verifying the message identification.

The validators should wait until the waiting time has passed, and if the n'-th node is first, it obtains a privilege of the block approval as a winner, which is expressed as

$$n' = \underset{i=1,2,\cdots,N;\ i\neq n}{\operatorname{argmin}} T_i^{k+1}, \qquad (1)$$

where T_i^{k+1} is the waiting time that obtains the i-th validator (i = 1, 2, ⋯, N; $i \neq n$). The winner node broadcasts the verified block with an identification and certification of the expired time, and then the other nodes append it to the BC. If two or more validators have won due to the same waiting time, the BC might fork. However, since the proposed scheme will be deployed in a (regional) smart-city area, thus we can ignore such situation because of sufficiently small scale.

In the network diagnosis, if the BC nodes are hijacked by attackers, those nodes will exhibit malicious verification, and the robustness of the BC will collapse. The proposed scheme selects the node that commits the verified block based on equal lottery. In addition, the group of malicious nodes are mutually privileged among them, so to analyze the history of the winner node in the BC, everyone can find them. As for the

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org

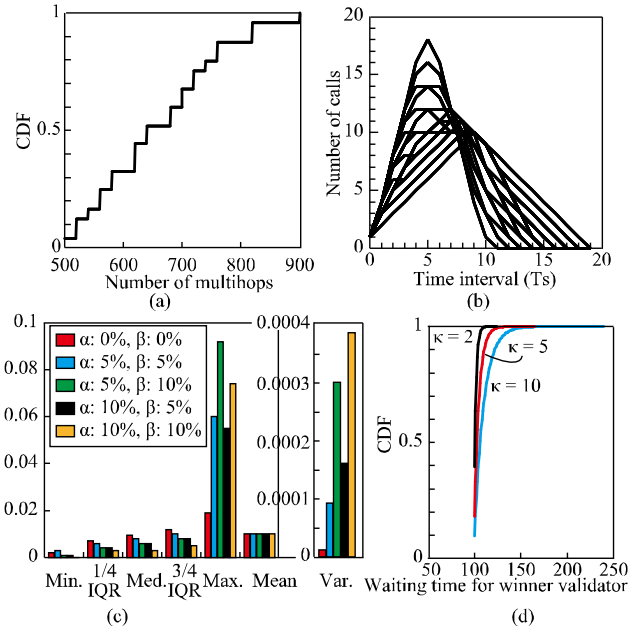

Figure 1. Numerical results

energy consumption of the network, the proposed scheme allows the validators to switch to idle or sleep states while waiting, thereby reducing both the computer resources required and the energy consumption.

III. NUMERICAL RESULTS

In this section, we present fundamental characteristics necessary for our scheme to work effectively and reduce energy consumption. Figure 1(a) shows the number of communications required for the request that the validators acquire a waiting time from the coordinator. The results were obtained through computer simulation implemented using C++. In the simulation, 100 lattice-like BC nodes were placed in a 1-km^2 field with 100-m separations. The results show the number of hops per node based on 10,000 block verifications, where the curve represents a statistical Cumulative Distribution Function (CDF). We found here that the request reached up to 6.60 hops per node and one-way direction on average. At the same time, even if a backhaul network has sufficient capacity, many requests will lead to congestion in the coordinator. For this situation, Figure 1(b) shows the number of call arrivals at the coordinator. The curves show the superimposed results of 100 trials. In the horizontal axis, T_s denotes the average time it takes for data to transmit between BC nodes. The results here show that the calls are centralized around five T_s, since the coordinator begins to accept requests and the coordinator maximally proceeds with 18 calls.

Figure 1(c) shows the distribution of the winner node based on the statistical values (minimum, 1/4 Interquartile Range (IQR), median, 3/4 IQR, maximum, mean, and variance values) related to the malicious node detection. α denotes the proportion of hijacked nodes to overall nodes, and β is the percentage at which the malicious nodes make the waiting time shorter among their member nodes. Note that the member nodes can be more likely to be selected as the next coordinator due to the shorter waiting time based on β. The simulation was performed for 1,000-block verification for combinations of α, and β was set to 0%, 5%, and 10%. In preliminary simulation, we performed the same evaluation for 1,000, 5,000, 10,000, 50,000, and 100,000 blocks, but there were no significant differences. As shown in Figure 1(c), on the basis of the maximum and variance values, the situation where the hijacked nodes are mixed can be detected. Figure 1(d) shows the CDF characteristics for the waiting time of the winner node, i.e., $T_{n'}^{k+1}$ in (1), in the case where $T_{\min}$ = 100 s and κ = 2, 5, and 10. These results are the average values after 1,000,000 trials. The waiting time was distributed based on a uniform distribution $\mathcal{U}(T_{\min}, \kappa N)$, where $T_{\min}$ is the predefined minimum time, N is the number of RNs, and κ is a constant value. As a result, the average verification times were 102 s, 104 s, and 109 s for κ = 2, 5, and 10, respectively.

On the other hand, regarding the comparison between block verification schemes, in general, a block verification scheme has three phases: block proposal, verification, and sharing. The block proposal and sharing phases are mostly the same procedure regardless of the consensus methods used. However, in verification phase, there is a significant difference in terms of whether a mining process is used (in PoWs) or a waiting process (in PoETs). In our previous study [4], we implemented a testbed device and measured the actual energy consumption as follows: 1.63 W (in sleep state), 2.76 W (in idle state), and 3.98 W (in computing state). Supposing the PoW and PoET consensus methods have the same processing time, the energy consumption can be reduced by 30.7% (during the idle waiting) and 59.0% (during the sleep waiting).

IV. CONCLUSIONS

In this paper, we proposed an energy-efficient PoET-based verification scheme. The computer simulations demonstrated the efficiency of the proposed scheme. In future work, we should discuss in-depth protocol design and evaluation.

ACKNOWLEDGEMENT

This work was partly supported by funding from Fukuoka University (Grand No. GW2309).

REFERENCES

[1] H. Asaeda, K. Matsuzono, Y. Hayamizu, H. H. Hlaing, and A. Ooka, "A survey of information-centric networking: The quest for innovation," *IEICE Trans. Commun.*, vol. E107-B, no. 1, pp. 139–153, 2024.

[2] B. S. Kim, C. Zhang, S. Mastorakis, M. K. Afzal, and J. Tapolcai, "Guest editorial special issue on information-centric wireless sensor networking (ICWSN) for IoT," *IEEE Internet of Things J.*, vol. 9, no. 2, pp. 844–845, Jan. 2022.

[3] C. Gündoğan, C. Amsüss, T. C. Schmidt, and M. Wählisch, "Content object security in the Internet of things: Challenges, prospects, and emerging solutions," *IEEE Trans. Network and Serv. Manag.*, vol. 19, no. 1, pp. 538–553, Mar. 2022.

[4] S. Mori, "A preliminary analysis of data collection and retrieval scheme for green information-centric wireless sensor networks," *Proc. ACM SIGCOMM 2022 WS NET4us*, Aug. 2022, pp. 1–6, doi: 10.1145/3538393.3544932.

Courtesy of IARIA Board and IARIA Press. Original source: ThinkMind Digital Library https://www.thinkmind.org