IARIA Congress 2024
(Porto, Portugal)

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

Shintaro Mori
(Fukuoka University)

福岡大學
FUKUOKA UNIVERSITY

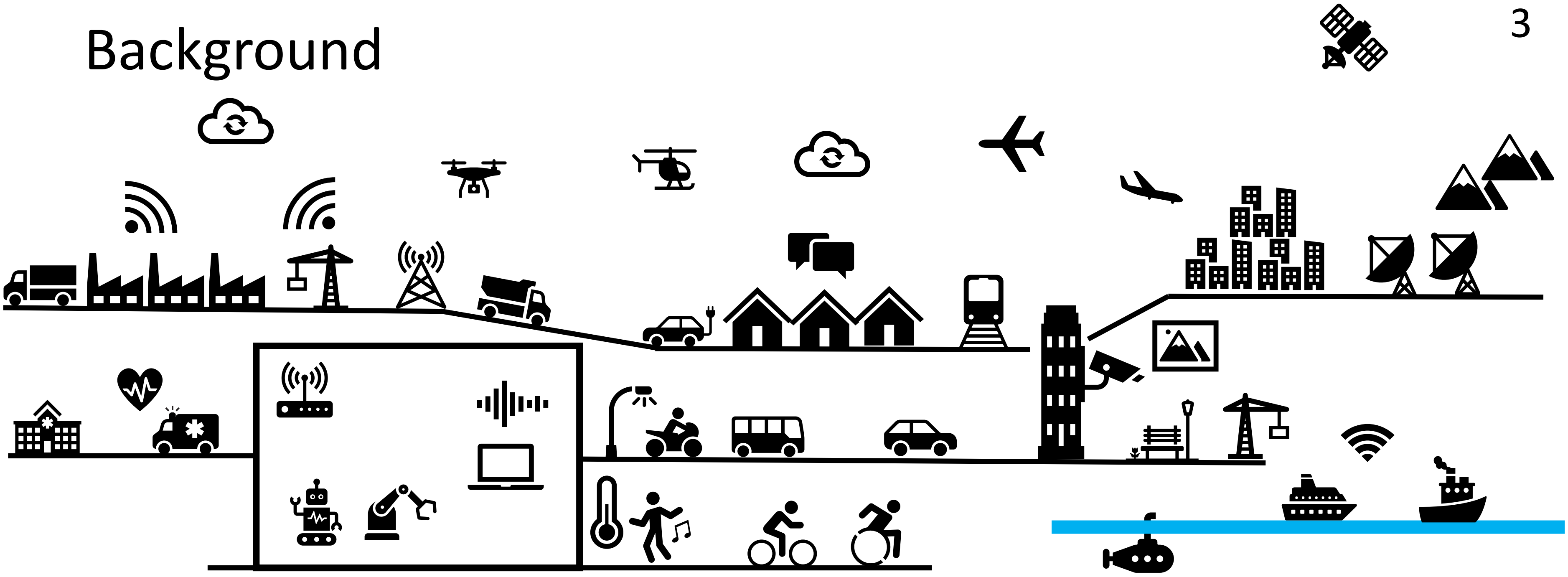
IARIA

Biography

Shintaro Mori received his B.S., M.S., and Ph.D. degrees from Kagawa University in 2007, 2009, and 2014, respectively. Since April 2014, he has been with the Department of Electronics Engineering and Computer Science, Faculty of Engineering, Fukuoka University, Japan, where he is currently an assistant professor. His research interests include cross-layer design, information-centric wireless sensor networks, and their application for smart cities. He is an IARIA Fellow and a member of IEEE, ACM, IEICE, ISSJ, and RISP.

- Topics of research interest:
  - Green information-centric wireless sensor networks (ICWSNs)
  - Smart-city applications for ICWSNs
  - Blockchains, unmanned aerial vehicles, or mmWaves for ICWSNs
  - Wireless sensor networks, body area sensor networks, and low-power wide area networks
  - Wireless communications and cross-layer design
- For more information, please see my website: https://www.cross-layer.com/

Background

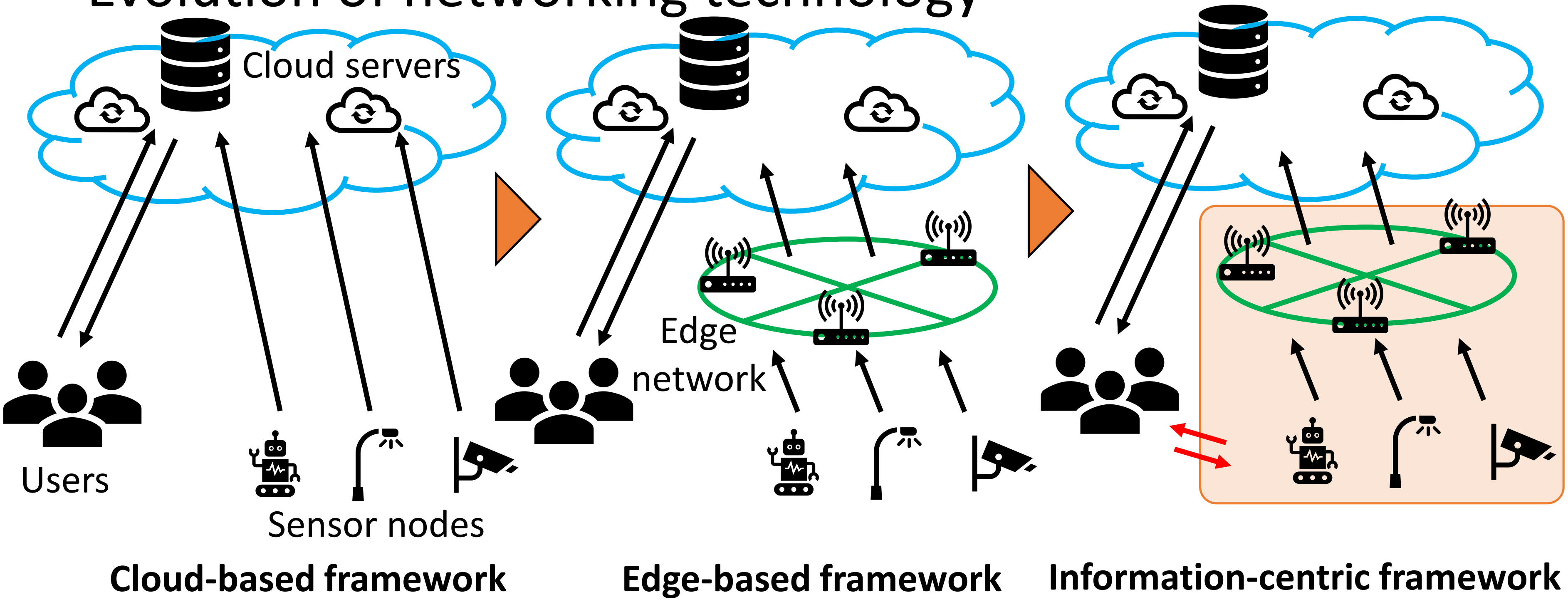


- Emerging technologies, such as the Internet of Things (IoT), metaverse, and artificial intelligence, enable crowd sensing in central city areas.
- Thanks to the massive amount of valuable information they provide, problems related to urbanization, social needs, and governmental structures can be mitigated.

▼

- Future wireless sensor network (WSN) technologies will provide essential functionalities for smart cities.

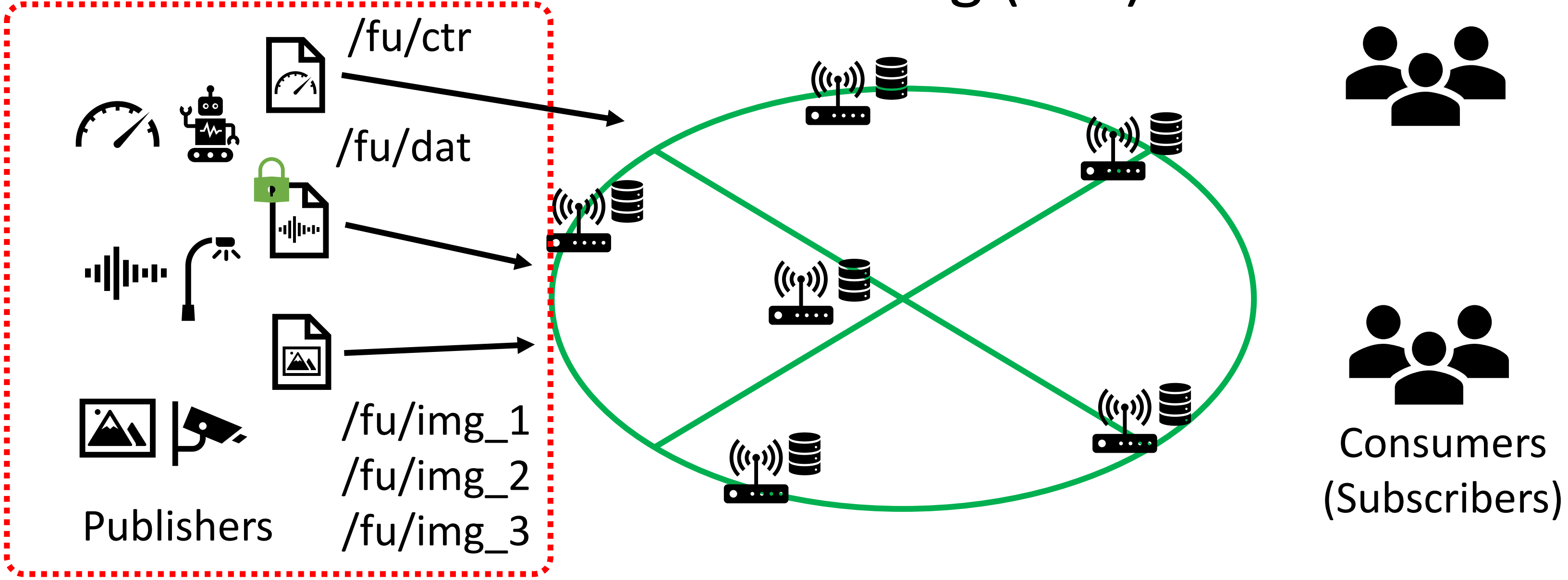
Evolution of networking technology



- 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] can be a promising solution.

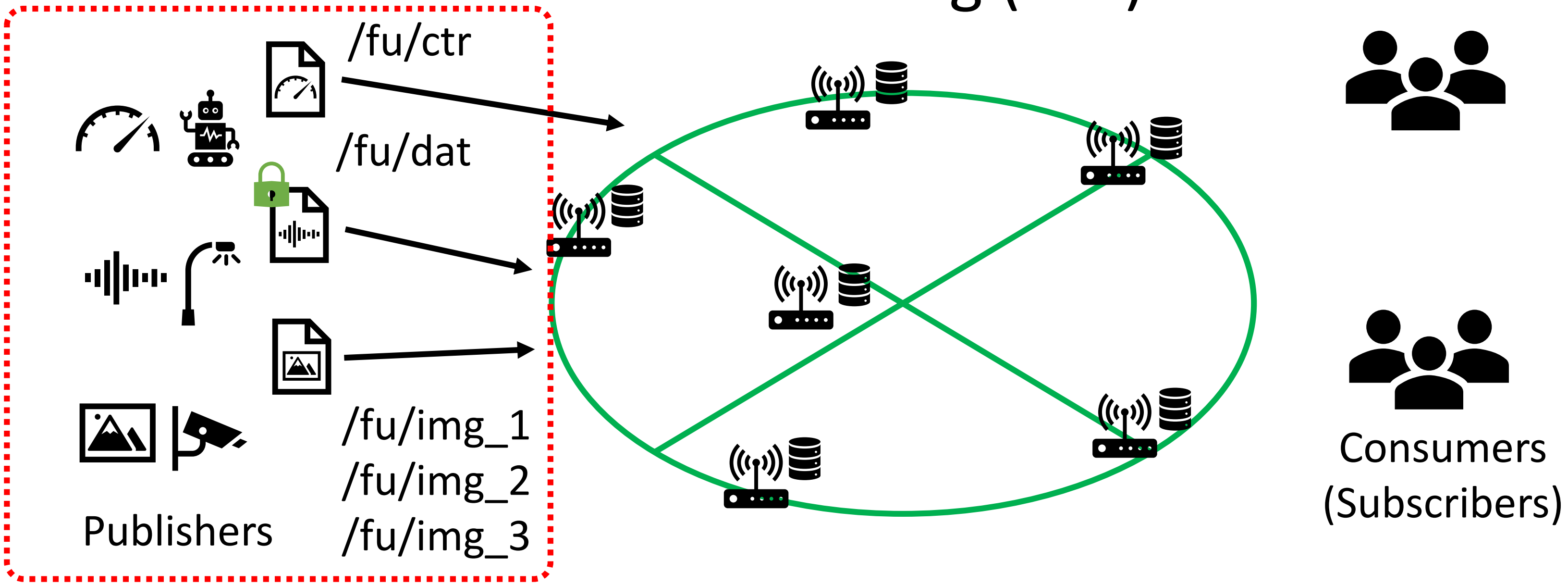
[1] H. Asaeda, K. Matsuzono, Y. Hayamizu, H. H. Hlaing, and A. Ooka, "A survey of information-centric networking: The quest for innovation," *IEICE Trans. Commun.*, vol. E107-B, no. 1, pp. 139–153, 2024.

Information-centric networking (ICN)



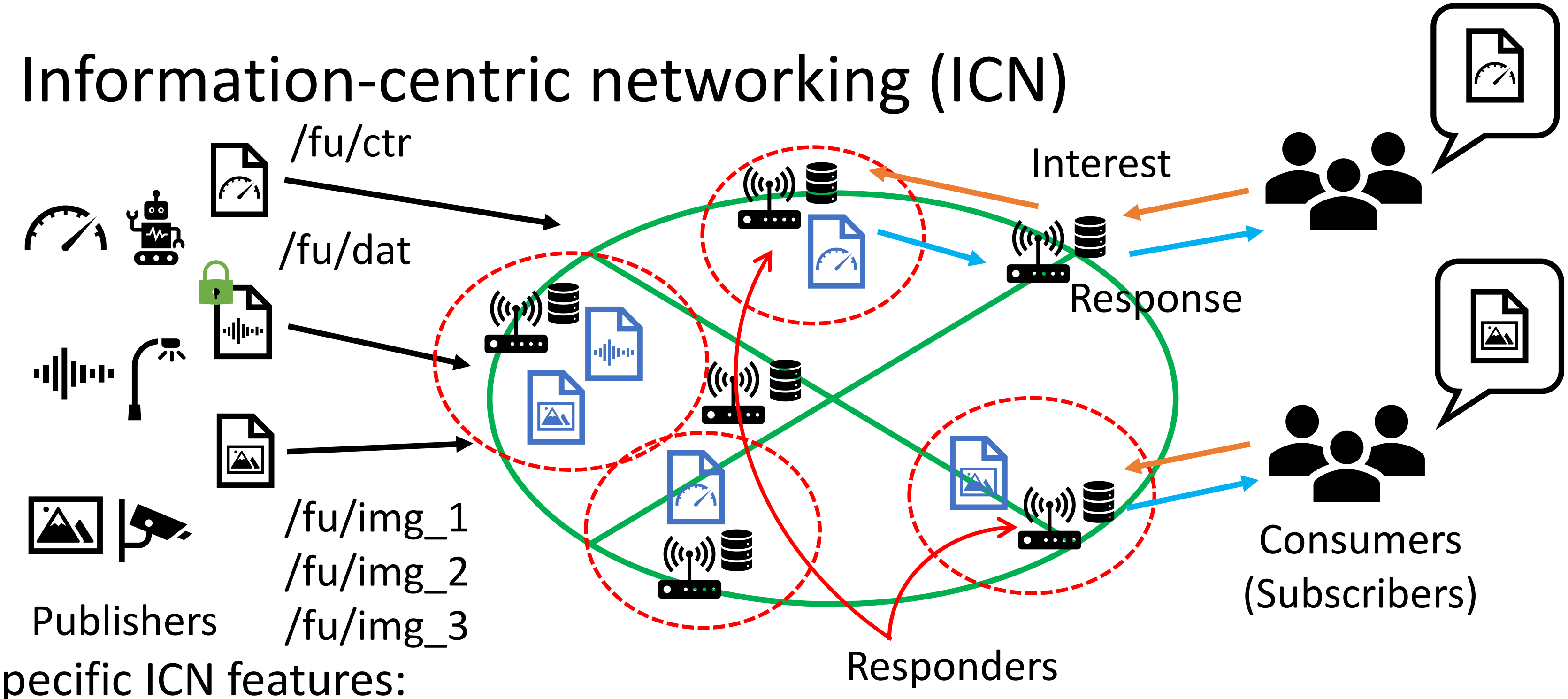
- ICN is a promising technology poised to replace the Internet architecture.
- ICN deals with the data as a named data object (NDO) for every piece of information, e.g., sensing data, images, videos, and other contents.
  - A large-data-size NDO can be divided into several chunks.
  - NDOs are detached from location, application type, and protocols.
  - The ICN protocol-tier security can be resolved for every NDO.
- ICN nodes provide an in-network caching for further effective responses.
- The features of ICN can boost location-free data access

Information-centric networking (ICN)



- Differences between ICN and the related technologies.
  - The search engines (or domain name systems) reply with the IP address for the keyword, and the users obtain the data based on the address.
  - Peer-to-peer (P2P) networks find the node with the data, and the user directly communicates with the node based on the address.
  - The content delivery network (CDN) technique is widely used to improve network congestion, especially in the area around the central servers.
  - Mirror-server framework is provided by cooperative servers.
- Users can obtain data from the geographically closest location.

Information-centric networking (ICN)



- Specific ICN features:
  - The data-transfer method is based on a multi-cast and multi-path network.
  - An in-network caching scheme is equipped; anyone can provide the data as long as they have it anytime and anywhere.
  - End-to-end connections should not be required, simplifying management, such as handover; the publishers and consumers can be decoupled.

- ICNs’ advantages:
  - Mobile publishers just submit the data to the network, and mobile consumers simply post the request for data retrieval to the network.
  - The smaller overhead for data exchange improves network congestion and latency, which can reduce wireless spectrum and energy consumption.

ICN + wireless (sensor) network + blockchain (BC)

- The combination of ICN and a wireless network is suitable, which yields information-centric wireless sensor networks (ICWSN) 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.

- The proposed scheme relaxes this limitation by using Blockchain (BC).
  - WICN with BC can provide a distributed, traceable, and immutable ledger without centralized and trusted nodes.
- The heavy burden is too much accepted for resource-constrained WICN nodes.
  - The data verification process must be performed iteratively for computer calculations, similar to the proof-of-works (PoWs) consensus method.
  - 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.

Proposed scheme

- Network construction
  - It is composed of a group of Sensor Nodes (SNs) and Relay Nodes (RNs).
  - Both of which are distributed across the local smart-city area.
- Network design
  - The proposed scheme overlays the BC on the WICN.
  - The role of the BC nodes is assigned to the RNs.

▼

- We utilize the Proof-of-Elapsed-Time (PoET) consensus method as a lightweight verification technique.
  - Each BC node is classified into one coordinator and several validators, with the coordinator providing a random waiting time to the validators.
  - Each BC node has a timer, and the first node for which a specified waiting time has elapsed is considered as a winner.
- 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.

Proposed scheme

- Assuming that
  - The winner node of the k th block (k = 0 means the genesis block) is the n th BC node ($n = 1, 2, \cdots, N$).
  - 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.
  - 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, as

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

T_i^{k+1} is the waiting time that obtains the i th validator ($i = 1, 2, \cdots, N;\ i \neq n$).

Proposed scheme

- The winner node broadcasts the verified block with an identification and certification of the expired time, and 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.
  - 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.
  - 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 energy consumption
  - 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.

Numerical results

- We present fundamental characteristics necessary for our scheme to work effectively and reduce energy consumption.
- Simulation environments
  - The computer simulators were implemented using C++.
  - In the simulation, 100 lattice-like BC nodes were placed in a 1-km^2 field with 100-m separations.
- Figure 1(a) shows the number of communications required for the request that the validators acquire a waiting time from the coordinator.
  - 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.
  - Even if a backhaul network has sufficient capacity, many requests will lead to congestion in the coordinator.

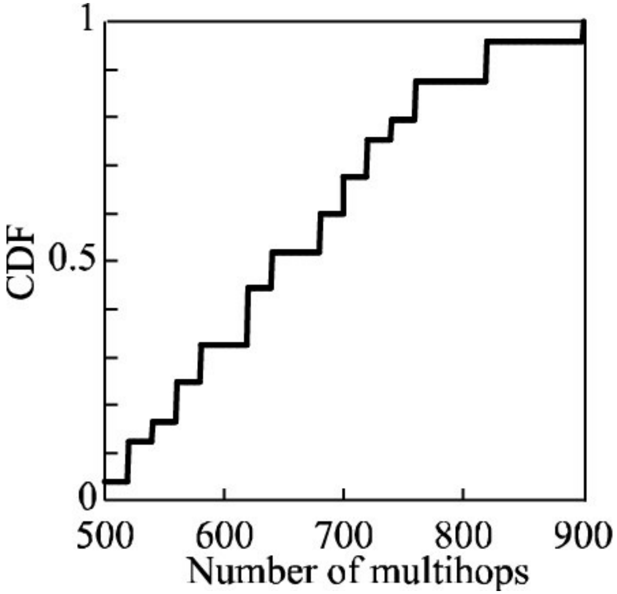


Figure 1 (a)

Numerical results

- Figure 1(b) shows the number of call arrivals at the coordinator.
  - Result is superimposed curves of 100 trials.
  - 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 5 T_s , since the coordinator begins to accept requests and maximally proceeds with 18 calls.

- Figure 1(c) shows the distribution of the winner node based on the statistical values.
  - α denotes the proportion of hijacked nodes to overall nodes
  - β denotes the percentage at which the malicious nodes make the waiting time shorter among their member nodes.
  - The simulation was performed for 1,000-block verification.

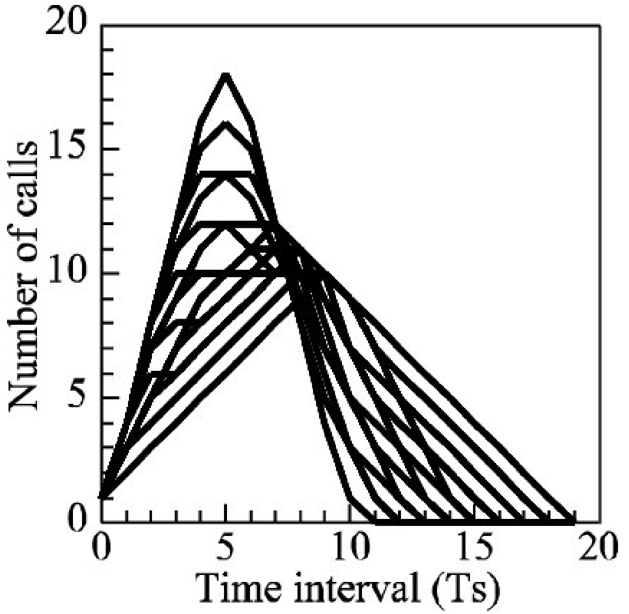
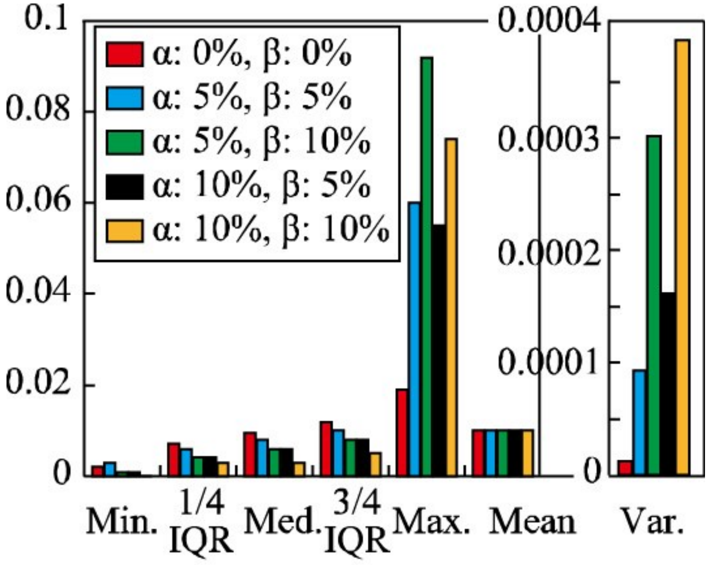


Figure 1 (b)



(c)

Figure 1 (c)

Numerical results

- Figure 1(c) shows the distribution of the winner node based on the statistical values.
  - 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.
  - On the basis of the maximum and variance values, the situation where the hijacked nodes are mixed can be detected.

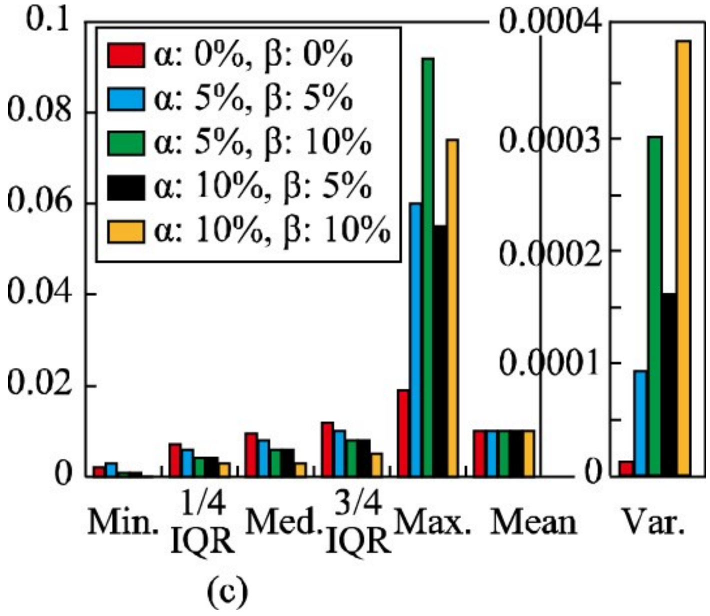


Figure 1 (c)

- Figure 1(d) shows the CDF for the waiting time of the winner node, i.e., T_i^{k+1} in (1).
  - These results are the average values after 1,000,000 trials.
  - The waiting time was distributed based on a uniform distribution $\mathcal{U}(T_{\min}, \kappa N)$.
  - The average verification times were 102s, 104s, and 109s for κ = 2, 5, and 10.

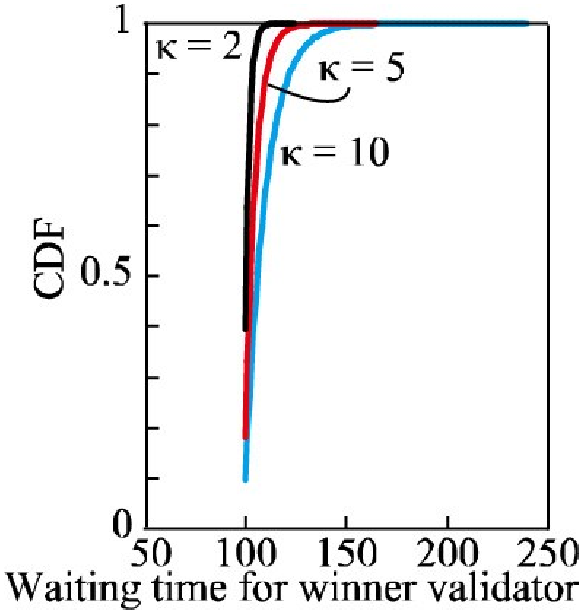


Figure 1 (d)

Numerical results

- As 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)
  - 3.98 W (in computing state).
- We assume that PoW and PoET have the same processing time, the energy consumption can be reduced by
  - 30.7% (during the idle waiting)
  - 59.0% (during the sleep waiting)

[4] Shintaro 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.

Conclusions

- Contributions
  - We proposed an energy-efficient PoET-based verification scheme.
  - The computer simulations demonstrated the efficiency of the scheme.

- Future work
  - We should discuss in-depth protocol design and evaluation.

Thank you for your attention.

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