Caching Data Protection Scheme for Information-Centric Wireless Sensor Networks

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— **Internet of things is widespread in our daily life, such as smart cities (homes), health care, and our activity lifelogs. In these use cases, sensing data must be managed not only effectively but also securely. From this perspective, we adopt the information-centric network design into wireless sensor networks for efficient peer-to-peer data collection, delivery, and publication. In the study of information-centric schemes, caching technology is significantly important; thus, we focus on a secure caching mechanism to privacy and security protections. In particular, the caching data protection mechanism, i.e., to prevent cache pollution attacks, is an essential challenge for data retrieving in information-centric wireless sensor networks. In this paper, therefore, we propose a novel effective and secure caching scheme for wireless sensor networks using the information-centric network design and the blockchain technology. In particular, for caching data management, to maintain the blockchain-based ledger requires exhaustive computer calculation resources and energy consumption in mining-based verification tasks; nevertheless, resource-limited wireless node devices are not suitable. Therefore, we propose a novel light-weight verification mechanism based on proof-of-consensus, and we reveal its fundamental features using computer simulation.**

Keywords-Wireless sensor network; Information-centric network; Blockchain; Caching scheme.

I. INTRODUCTION

The growing number of devices connected to the Internet has made the ubiquitous Internet a part of all aspects of modern life. Countless new Internet-of-Things (IoT) devices are widely used by smart cities/homes, healthcare services, and other sensor and actuator solution providers. Future IoT systems are expected to communicate with each other directly, sending and receiving an enormous amount of sensing data (Figure 1). These privacy-sensitive sensing data have been under various attacks in the already deployed terminals, causing serious security concerns [1]. For example, if smart city applications are hacked and users' activities are leaked, people's personal safety can be compromised. In another example, if healthcare and smart medical devices for fitness, diet, and health monitoring do not work adequately, emergency notifications and early detection of illnesses cannot be sent. That is why Wireless Sensor Networks (WSNs) in key wireless technologies underpinning IoT services should evolve and be replaced by a modern autonomous, decentralized, efficient, secure, and privacy-aware network design. These concerns motivated us to develop an effective and secure data management scheme (including storing, forwarding, and providing) based on Information-Centric Network (ICN) design and blockchain technology. In comparison with the traditional scheme, the proposed scheme has a significant characteristic and advantage that the proposed scheme can be constructed based on an overall distributed and decentralized design due to a combination of WSNs, ICN, and blockchain.

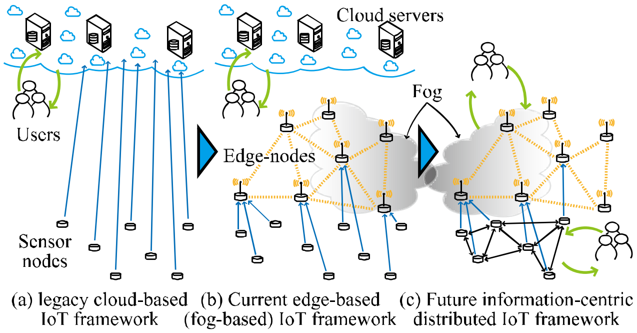
Cloud servers
Users
Fog
Edge-nodes
Sensor nodes
(a) legacy cloud-based IoT framework
(b) Current edge-based (fog-based) IoT framework
(c) Future information-centric distributed IoT framework

Figure 1. Transition of IoT framework architecture.

The ICN is emerging as a promising network architecture that supports efficient data provision and retrieval with in-network caching, i.e., users could obtain their desired content data from a nearby copy-holder in ICN-based systems [2]. To initiate this mechanism, users send a content request with the desired content feature in an interest packet; then, the content is sent back to the requester in a data packet when the interest packet reaches the original node or cache-available node. The reason for introducing ICN into WSNs is that the address-free structure is suitable for mobile and ad-hoc network environments, allowing ICN-WSNs to reduce the protocol overhead of data collection and retrieval in comparison with HTTP and other simplified protocols [3]. In implementation of ICN-WSN systems, the caching scheme is one of the essential technologies in the ICN framework, resulting in failed cache poisoning attacks due to the actuators performing wrong actions founded on the polluted data.

To protect the caching data of ICN-WSNs, we use the blockchain technology [4]. These three key technologies, the

WSN, the ICN, and the blockchain, work in an autonomous and decentralized environment. A blockchain-based ledger has several advantages: it can be constructed among anonymous nodes; the verification process is simple and common manner; the users can easily identify and authenticate the verified caching data without central brokers or certification authorities, and the blockchain architecture protects it from the risk of being a single point of failure when faced with malicious attacks. Moreover, when a verified block is appended into the blockchain, the users do not need any additional certification process.

A typical blockchain verification process needs exhaustive computer calculations called Proof-of-Work (PoW). Such PoWs are used, for example, by Bitcoin [5] and other crypto-currencies but cannot be applied in ICN-WSNs consisting of cheap and resource-constrained devices. Even if the proposed scheme will utilize movable vehicle nodes, such as drones and small vehicles, for data collection, accumulation, and provision, the hardware limitations can be alleviated, but the essential issues will remain. Unlike PoWs, Proof-of-Stake (PoS) utilized in Ethereum [6] does not require heavy-weight computational operations, i.e., the next block generator is selected in a pseudo-random way. However, the verification task depends on the wealth or stake of a node, i.e., the more money the node has, the higher its chances for validation, making some nodes unbalanced.

To mitigate these problems, we investigate a novel blockchain-based secure caching and data retrieving scheme for ICN-WSNs. In particular, we propose a novel light-weight verification scheme where blocks are verified while relay nodes forward unverified blocks in ad-hoc and multi-hop networks among validators in the usual WSN data transfer. In this paper, we describe the overall blueprint of our work in progress and propose a novel verification mechanism. We perform a fundamental evaluation of the proposed mechanism using computer simulation.

The remainder of this paper is organized as follows. Section II provides related work. Section III describes the proposed scheme. Section IV presents the numerical results. Finally, in Section V, we summarize our findings and conclude the paper.

II. Related Work

In legacy cloud based IoT frameworks, the authentication, authorization, and access control methods are applicable and selected as centralized controllers that currently deal with these services. While WSN systems are shifting towards decentralization, as in the edge-computing and the fog-computing, alternative security mechanisms for authentication, confidentiality, privacy, access control, resource provenance, and integrity are required [7]. Blockchain technology can address various security issues by constructing a secured and distributed ledger. Alphand et al. [8] proposed a combination scheme of the authorization blockchain and the group key for providing secure-authorized access to IoT resources. From the viewpoint of ICN caching data protection, several studies should be mentioned. Li et al. [9] proposed a blockchain-based protection scheme of the data life cycle; Guo et al. [10] investigated a public permissionless blockchain in named data networking, and Li et al. [11] proposed a trust-enhanced blockchain-based ICN architecture for content delivery.

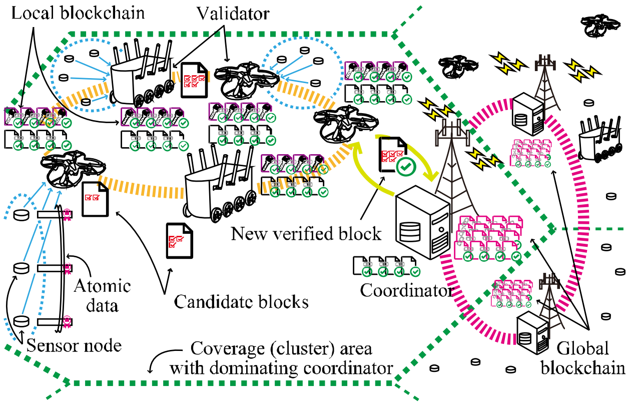

Figure 2. Overview of the proposed scheme.

On the other hand, in wireless networks, Liu et al. [12] proposed a mobile edge-computing-enabled wireless blockchain framework where the computation-intensive mining tasks and verified blocks can be offloaded and cached to neighboring nodes. Chai et al. [13] and Sharma et al. [14] suggested replacing fixed terminals with mobile (aerial) vehicles. These proposals represent an evolution in the content delivery network; however, they are still far from adopting the ICNs in WSNs. In other words, the conventional approach places the content servers in the mobile-edge nodes, which is different from the ICN principle of an individual node copying and storing the caching data. Similar to our study, Lei et al. [15] proposed a novel and systematic framework to protect the in-network caching mechanism; it enables fast and efficient content dissemination in mission-critical ad-hoc networks. However, this proposal has a drawback in that it involves an exhaustive verification process, the proposed scheme can improve the burden of verification calculations.

III. Proposed Scheme

In the data life cycle of ICN-WSNs, the atomic data collection, caching, and retrieval processes may suffer from various attacks. The ultimate goal of our study is to develop an anti-tamper caching scheme.

A. System Description

In the proposed scheme, Sensor Nodes (SNs) are massively deployed in the observation field, which is divided into several regions and the segmented area has one coordinator for comprehensive management, as shown in Figure 2. There are four network components, and the entities that logically play roles in content data dissemination are as follows.

- *SNs* periodically generate atomic data that is a data unit of the ICN content.
- *Validators* gather atomic data from SNs and summarize them into a block that is a data unit of the blockchain. Validators are implemented using

movable nodes, such as drones and small vehicles, and blockchains are constructed on them. Validators have less hardware limitations compared with SNs.

- *Coordinators* decide which block to append into the blockchain among verified blocks. Coordinators mediate between regional blockchains and global blockchains to achieve scalable data retrieval.
- *Users* behave as subscribers, i.e., send data retrieval requests, such as interest requests, to validators and obtain data from the original content or the caches in the validators' blockchain network.

In the proposed scheme, blockchains can be functionally systematized as local blockchains and global blockchains. Local blockchains manage not only the atomic data but also the validity keys for atomic data verification. Thus, coordinators exchange the extracted and summarized information of verified blocks between the global blockchain and the local blockchain of the atomic data to share inventory. Namely, they produce knowledge data, which refers to the data summarized from the local blockchain, including the atomic data, signature, meta tag information necessary for the ICN search. By adopting this mechanism, users can obtain content data from the cross-sectional observation areas. Although the implementation cost occurs to introduce a blockchain-based ICN's caching mechanism into WSNs, we believe that it would be a move well worth the cost because blockchain-based ledgers can also use extensive solutions, such as certification key protection, user access control, and resource management.

B. Verification Procedure

Before entering into a block certification process, when the SN joins in and connects to the WSN, a secret key should be provided in order to sign an atomic data digitally. As shown in Figures 3 and 4, in the initialization process, the new SN sends a request for its secret key provision to the neighboring validator (①), and then the validator generates a public key, $\mathcal{PK}$, for validation and a secret key, $\mathcal{SK}$, for signature (②). $\mathcal{PK}$ is appended to the validation key's blockchain (③) and $\mathcal{SK}$ is provided to the SN (④).

In the proposed scheme, there are three types of blocks: a candidate block, a verified block, and a chained block. Candidate blocks that have not yet been verified are generated by collecting and summarizing several atomic data (⑤). Besides, candidate blocks include not only the atomic data but also header parts, such as meta-data for ICN retrieval, as well as a sequential number and a unique fingerprint to distinguish one block from another. The reason for using both the sequential number and the unique fingerprint is that the same sequential number cannot be allocated to different candidate blocks.

Candidate blocks are cross-verified based on Proof-of-Consensus (PoC) used in Ripple [16]. In the proposed validation process (⑥), if a candidate block obtained the sufficient consensus of almost all reliable validators, it can be regarded as a correctly verified block. In the event that a number of validators are hijacked and an illegal validation is carried out, the proposed scheme will maintain the robustness of the blockchain tanks to the distributed verification feature. The proposed scheme does not require exhaustive mining-based computer calculations for block verification; hence, it is suitable for resource-scarce WSN environments. Candidate blocks are exchanged based on multi-hop wireless transmissions among validators (edge-nodes or fog nodes), i.e., the candidate block can gain the consensus of validity during data forwarding. Note that in the validation process, extra-data transmission with the proposed validation mechanism does not occur. The validator can approve the validity of the atomic data using $\mathcal{PK}$ based on the public key cryptosystem technique (in particular, the digital signature method) to guarantee the integrity and authenticity of the candidate blocks.

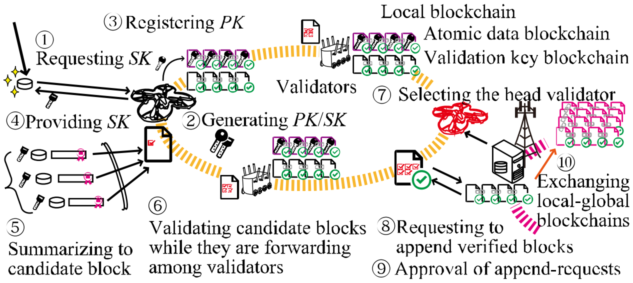
③ Registering PK
① Requesting SK
④ Providing SK
② Generating PK/SK
Local blockchain
Atomic data blockchain
Validation key blockchain
Validators
⑦ Selecting the head validator
⑩ Exchanging local-global blockchains
⑤ Summarizing to candidate block
⑥ Validating candidate blocks while they are forwarding among validators
⑧ Requesting to append verified blocks
⑨ Approval of append-requests

Figure 3. Procedure of the proposed validation process and appending verified blocks into blockchains.

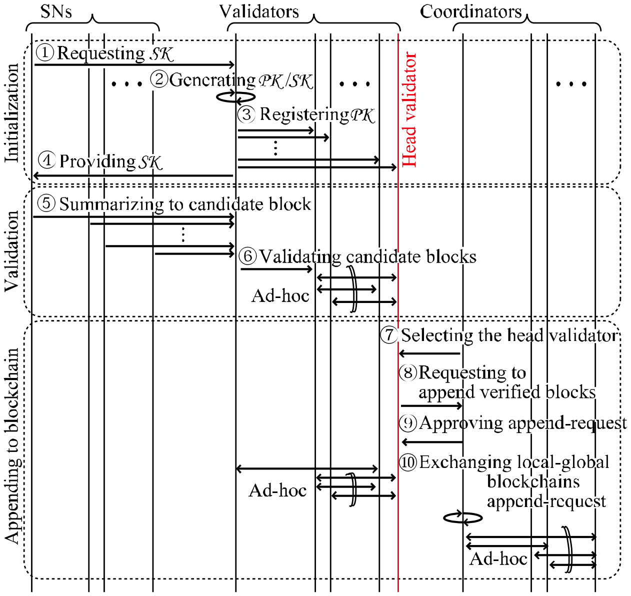
SNs
Validators
Coordinators
Initialization
Validation
Appending to blockchain
Head validator
① Requesting $\mathcal{SK}$
② Generating $\mathcal{PK}/\mathcal{SK}$
③ Registering $\mathcal{PK}$
④ Providing $\mathcal{SK}$
⑤ Summarizing to candidate block
⑥ Validating candidate blocks
Ad-hoc
⑦ Selecting the head validator
⑧ Requesting to append verified blocks
⑨ Approving append-request
⑩ Exchanging local-global blockchains append-request
Ad-hoc
Ad-hoc

Figure 4. Message and data flow of the proposed scheme.

The coordinator selects the head (representative) validator (⑦), which will be the nearest validator to the coordinator to avoid complexity in this paper. The head validator selects a new chained block (that might not necessarily be appended to the blockchain) among the verified blocks within its cache memory. Namely, the head validator sends a request of the verified block appending to the coordinator (⑧), and the coordinator approves the request if there are no complications (⑨). In addition, the coordinator calculates a new hash value of the final and fixed chained blocks, instead of a fingerprint in candidate block, consensus information, and the previous block's hash value. In updating the local atomic data's blockchain, the renewal chained block is copied, stored, and cached among validators. Moreover, the coordinator summarizes the inventory of the chained blocks and shares the information with the outside coordinator networks. When the current head validator has no more verified blocks or goes out of the coordinator's coverage, the current head validator swaps with a new one that the coordinator re-selects. Note that the position and the privilege of the head validator are rotated among validators because validators move with time; therefore, we expect that verified blocks are uniformly and fairly appended into the blockchain.

IV. Computer Simulation

In this section, we provide fundamental analysis prior to the demonstration in a realistic environment and to compare with other related schemes in our future work. Computer simulator is implemented using C++ language and its program code is run on PC (Windows 10 OS, Intel Core i5-9400 CPU, and 16 Gbyte RAM).

Figure 5 illustrates how many validators are necessary to communicate with all the SNs in the observation area (400 km^2 square) and how many SNs does one validator dominate: 4,000,000 SNs are deployed in an equally-spaced grid pattern, and validators are placed randomly. We assume that the radius of circular-shaped wireless communication coverage between the SN and the validator is set to 1 km, and we ignore the shadowing and the fading depending on the validator's mobility, ground surface, and radio propagation conditions to avoid complexity in the analysis. As a result, 95% of SNs and 98% of SNs can be covered by 400 and 500 validators, respectively. In addition, a scheme for interference reduction should be considered because multiple validators cover almost all SNs. Although the communication range should be small to avoid interference among validators and reduce energy consumption, numerous multi-hops forwarding among validators is necessary for the success of block validations.

Figure 6 shows a relationship between the probability of the validation being completed (and the number of the multi-hops necessary for it) and the communication range. As a result, 95% of blocks can be successfully validated when the communication range is 4 km and the candidate block is forwarding more than four times. In the case when the radius of communication area is large, the number of communications for sufficient consensus becomes small, i.e., the average number of multi-hops also becomes small. On the basis of this scenario, Figure 7 shows the tolerance for caching data pollution, i.e., the number of maliciously taken validators and illegally accepted verified blocks. For example, when the number of maliciously hijacked validators is 1%, 2%, and 3%, the probability of wrongfully verified block is 3.21%, 7.66%, and 12.6%, respectively.

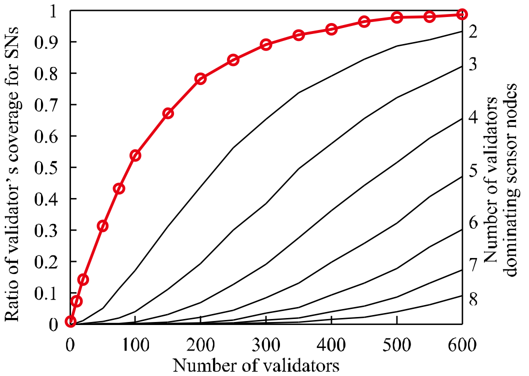

Figure 5. Validators coverage for SNs versus number of validators.

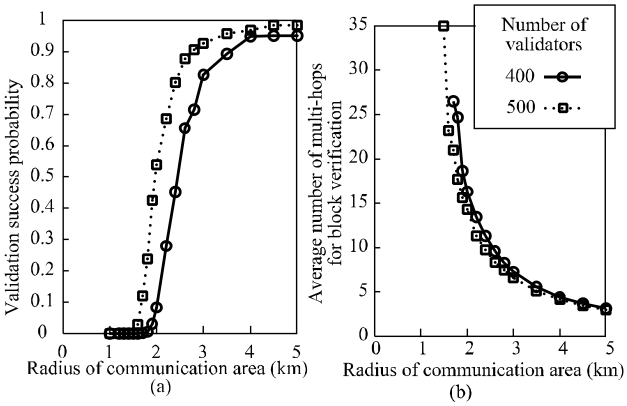

Figure 6. a) Probability of validation being completed and b) average number of multi-hops for block verifying versus radius of communication area between validators.

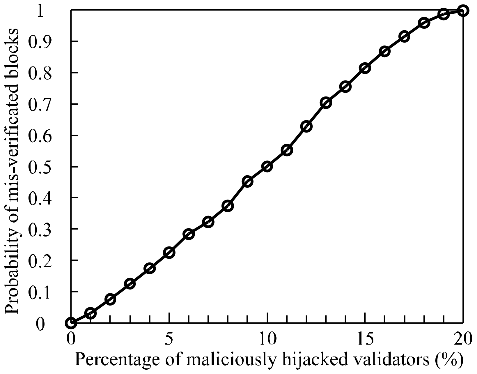

Figure 7. Probability of wrongfully verified blocks versus percentage of maliciously hijacked validators

V. Conclusion

In this paper, we adopted the ICN design into WSNs for efficient peer-to-peer data collection, delivery, and publication, and we focused on a secure caching mechanism to privacy and security protections. In order to achieve them, we proposed a novel effective and secure caching scheme using blockchain technology in order to prevent cache pollution attacks. In particular, we proposed a novel light-weight verification mechanism based on proof-of-consensus, and we reveal its fundamental features using computer simulation. As future work, we will consider a data retrieval mechanism based on global blockchain and an incentive mechanism, such as a reward in Bitcoin, and evaluate them using comprehensive simulations.

Acknowledgment

A part of this work was supported by JSPS KAKENHI Grant Number JP19K20261.

References

[1] V. Hassija, et al., “A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures,” *IEEE Access*, vol. 7, pp. 82721–82743, 2019.

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, “A Survey of Information-centric Networking,” *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 26–36, July 2012.

[3] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, “Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT),” *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2128–2158, Apr. 2019.

[4] K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” *IEEE Access*, vol. 4, pp. 2292-2303, 2016.

[5] S. Nakamoto, “Bitcoin: A Peer-to-peer Electronic Cash System,” *Tech. Rep.*, 2008.

[6] Ethereum, https://www.ethereum.org/ [retrieved: Jan. 2020].

[7] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, “Security Services Using Blockchains: A State of the Art Survey,” *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 1, pp. 858–880, First-quarter 2019.

[8] O. Alphand et al., “IoTChain: A Blockchain Security Architecture for the Internet of Things,” *Proc. 2018 IEEE Wireless Commun. and Networking Conf. (WCNC’18)*, Feb. 2018, pp. 1–6, doi: 10.1109/WCNC.2018.8377385.

[9] R. Li and H. Asaeda, “A Blockchain-Based Data Life Cycle Protection Framework for Information-Centric Networks,” *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 20–25, June 2019.

[10] J. Guo, et al., “Enabling Blockchain Applications Over Named Data Networking,” *Proc. IEEE Int. Conf. Commun.(ICC’19)*, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761919.

[11] H. Li, et al., “Trust-Enhanced Content Delivery in Blockchain-Based Information-Centric Networking,” *IEEE Network*, 7 pages (in press).

[12] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung, and M. Song, “Computation Offloading and Content Caching in Wireless Blockchain Networks with Mobile Edge Computing,” *IEEE Trans. Vehicular Tech.*, vol. 67, no. 11, pp. 11008–11021, Nov. 2018.

[13] H. Chai, S. Leng, M. Zeng, and H. Liang, “A Hierarchical Blockchain Aided Proactive Caching Scheme for Internet of Vehicles,” *Proc. 2019 IEEE Int. Conf. on Commun. (ICC’19)*, May 2019, pp. 1–6, doi: 10.1109/ICC.2019.8761482.

[14] V. Sharma, I. You, D. N. K. Jayakody, D. G. Reina, and K. R. Choo, “Neural-blockchain based Ultra-reliable Caching for Edge-enabled UAV Networks,” *IEEE Trans. Industrial Informatics* (in press).

[15] K. Lei, Q. Zhang, J. Lou, B. Bai, and K. Xu, “Securing ICN-Based UAV Ad Hoc Networks with Blockchain,” *IEEE Commun. Mag.*, vol. 57, no. 6, pp. 26–32, June 2019.

[16] Ripple, http://ripple.com/ [retrieved: Jan. 2020].