Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 3027978, 13 pages
https://doi.org/10.1155/2022/3027978

Research Article

Design and Implementation of Ledger-Based Points Transfer System for IoT Devices in LPWAN

Xin Qi[1], **Keping Yu**[2], **Toshio Sato**[1], **Kouichi Shibata**[3], **Isao Konno**[3], **Takanori Tokutake**[4], **Rikiya Eguchi**[4], **Yusuke Maruyama**[4], **Zheng Wen**[4], **Kazuhiko Tamesue**[1], **Yutaka Katsuyama**[1], **Kazue Sako**[4], **and Takuro Sato**[1,4]

[1]*Global Information and Telecommunication Institute, Waseda University, Shinjuku, Tokyo, Japan*
[2]*Graduate School of Science and Engineering, Hosei University, Tokyo, Japan*
[3]*Skeed Co., Ltd., Tokyo, Japan*
[4]*School of Fundamental Science and Engineering, Waseda University, Tokyo, Japan*

Correspondence should be addressed to Xin Qi; samqixin@aoni.waseda.jp

Received 28 April 2022; Revised 28 May 2022; Accepted 12 July 2022; Published 19 August 2022

Academic Editor: Huimei Han

Distributed ledger technology is becoming popular these days because of its high confidentiality, decentralization, and nontampering. It is suitable for replacing centralized security disadvantaged point transfer systems. Low-power wide area network (LPWAN) is capable for long-range communication with low-power consumption. The iconic features like wide area coverage and long battery-powered duration make it best to combine with large-scale IoT application deployment. In both industry and academic field, such combination of LPWAN and point transfer system is highly attended. However, the ledger management system generates too much data that low-bandwidth network such as LPWAN can hardly handle; meanwhile, the processing power's requirement for small IoT devices is challenging. Towards addressing these issues, we design a packet transmission optimizing mechanism for a ledger-based point transfer system (LPTS) in LPWAN to reduce overall data traffic and build a simulator to evaluate its performance. Moreover, we have implemented the system and evaluated in field experiment.

1. Introduction

The current demand of information and communication technology has changed from simple point-to-point communication to interconnection of people and things and things and things and eventually realizes the interconnection of everything. In the process of upgrading and iterating mobile communication technologies, branches that focus on low-power communication technologies, such as Bluetooth, ZigBee [1], and other short-range communication technologies, have also developed. However, with the development of the Internet of Things (IoT), a large number of devices need to be interconnected, and their communication requirements are based on low mobility, low communication frequency, and low data volume. Traditional wired communication technologies are clearly not adaptable. Short-range communication technology cannot provide enough communication distance to meet the demand of long-distance and wide coverage of IoT. Mobile cellular networks, which are based on high speed, wide coverage, high mobility, and high terminal capacity, also discourage IoT. To solve this problem, an IoT network access technology with low cost, wide coverage, and simple deployment, and support for large number of connections, low-power wide area network (LPWAN) [2], has emerged. LPWAN-based interconnection systems are gaining widespread attention from academia and industry [3]. LPWAN has formed several technology camps worldwide, including narrow-band Internet of Things (NB-IoT) [4, 5], Long Range Wide Area Network (LoRaWAN) [6–8], Sigfox [9–11], and weightless [12].

Meanwhile, modern information technology represented by the Internet, especially mobile payment, has had a fundamental impact on the human financial model. Along with the invention of digital currencies, the evolution of ledger

technology can address the security issues of centralized services [13]. In other words, a ledger is similar to a database holding assets that can be shared across multiple sites, different places, or networks. Moreover, a decentralized ledger is designed to guarantee for tamper-proofing and being encrypted. It is currently most widely used in IoT finances. However, a traditional point transfer system is usually based on a centralized computer system with powerful processors, which consume much energy. When a point transfer system is introduced in a decentralized system, it is hard to simply split the computing need to individual nodes in the network. The combination of sensing, communication, and computing (SCC) needs to be smart deployed in the network. In other words, a more suitable design is needed for decentralized ledger systems to satisfy low-power hunger IoT devices. The specific contributions are as follows.

(1) This paper designs a lightweight ledger-based point transfer system (LPTS) in LPWAN, which can guarantee the data security well and is suitable for IoT devices with weak computational power and capacity

(2) A field experiment is performed to evaluate the implementation of the system

(3) Additional signatures and an optimal packet delivering algorithm is proposed and evaluated by simulations. Evaluation against disasters is also performed

The rest of this paper is organized mainly into three parts as follows. In Section 2, we describe the related work on LPWAN, ledger-based technology for IoT, and other lightweight distributed ledger system. In Section 3, we describe the design of LPTS with its principle, algorithm, configuration, and evaluation. Section 4 describes the implementation of LPTS with module designs and working prototype. Section 5 describes the extension of LPTS to improve either its security, packet transmission, or disaster management. Finally, we conclude the paper in Section 6.

2. Related Works

In the recent years, IoT had been a top trending field, and LPWAN is also a hot wireless technology that was introduced for IoT. On the other hand, Wi-Fi [14], ZigBee [15, 16], and Bluetooth technologies are dedicated high speed and low communication frequency, not very suitable for those battery-powered and long range communication needed IoT devices. In LPWAN field, NB-IoT is built by telecommunication operators with the adoption of cellular communication technology and authorized frequency bands [17, 18]. LoRa works in an unlicensed frequency band with linear spread spectrum technology, which is setup and managed by users [19, 20]. ZigBee mainly focuses on home IoT devices which use common frequency band. Table 1 shows some specifications of the above communication technologies. NB-IoT and LoRa perform the best in power consumption, up to 10 years with AA battery. However, the transmission data rate is too low to handle real-time data [21] in monitoring scenarios.

Most IoT devices rely on the centralized servers or cloud servers to actually communicate with other devices [22]. It was possible to use satellite communication-based cloud service for remote nodes [23], but the power consumption was too high. In some studies, Proof-of-Work (PoW) [24] principle still suffers from 51% attack [25]. Centralized management can offer easy management and accesses but can also cause privacy and security issues, then comes the distributed ledger technology and IoT-powered integration. IoT devices can exchange, store, and generate data by using peer-to-peer technology, which is a characteristic role in distributed ledger systems [26]. This can ensure its privacy and robustness. Creating, modifying, and deleting data can be verified in IoT-powered distributed ledger to detect and prevent data misuse and tampering [27, 28].

3. Design of Ledger-Based Points Transfer System for IoT Devices in LPWAN

3.1. Design Principle. The design principle of LPTS for IoT devices in LPWAN is listed as below and referenced in Figure 1:

(1) Realize point transfer from A to B. The client can be terminals or other user devices

(2) The ledger management can manage the point balance of each user. The ledger should be tamper-proof

(3) LPWAN applied to achieve system availability even in the event of a disaster (achieved in Section 5)

(4) Packet delivery mechanism optimization applied to achieve high packet deliver rate even with low communication bandwidth of LPWAN (achieved in Section 5)

(5) System should be able to implement into IoT devices and be evaluated in field experiment

The main purpose of the point transfer system is to realize the function that delivers points from A to B. The users can use their terminal devices like smartphones or integrated devices. The user sends a point transfer request to the network, and the ledger management should be able to verify and start the point transfer process. After the point transfer, the point balance of the sender and receiver should be kept recorded in the ledger system; a certain way of validation should be implemented in the ledger system to protect it from tampering. Because this system has its application in disaster scenarios like earthquakes and tsunamis, it is important to make the nodes to run with battery power and wide area coverage. LPWAN is suitable for these situation and selected for the communication network for the point transfer system. However the bandwidth that LPWAN provides is known to be quite low comparing with modern cellular network or Wi-Fi. A packet delivery mechanism is proposed to optimize the bandwidth consumption, letting the network be valid and fast. Small-scale IoT devices like ARM-based chip sets are known to be energy saving and are suitable to hold

Table 1: Comparison of wireless communication technologies.

Technology	Frequency	Transmission rate	Transmission distance	Maximum support nodes	Power consumption (AA battery)
LoRa	150 MHz-1 GHz	0.3-50 kbps	~ 15 km	200000	About 10 years
NB-IoT	Operator bands	<100 kbps	10-15 km	200000	About 10 years
ZigBee	2.4 GHz	<250 kbps	10-75 m	65000	About 2 years
Bluetooth	2.4 GHz	<1 mbps	20-200 m	7	Weeks
Wi-Fi	2.4/5 GHz	<54 mbps	20-200 m	2007	Hours

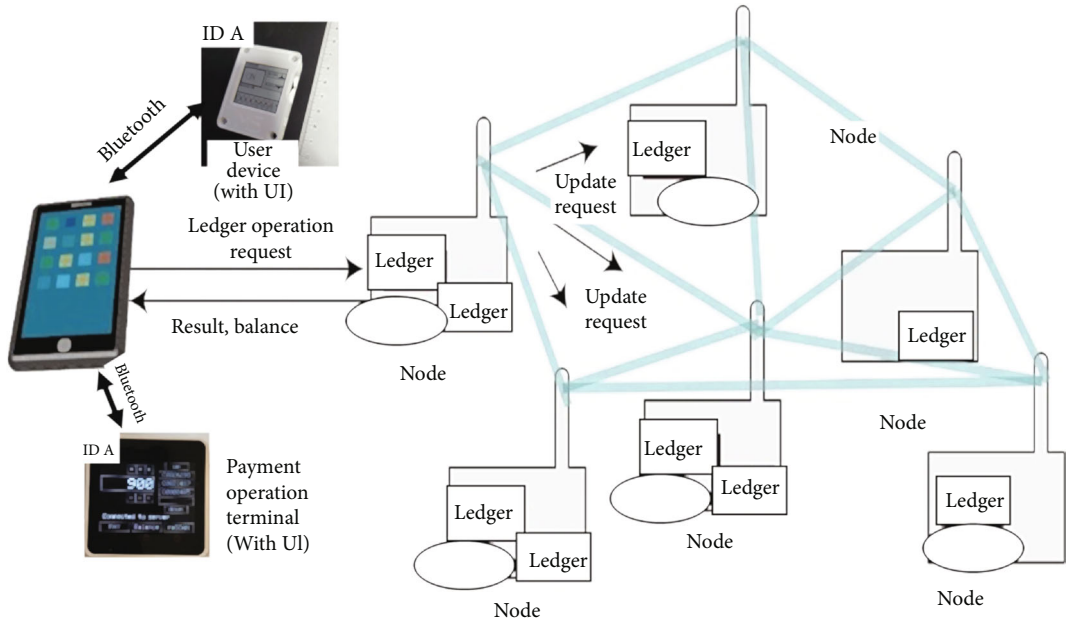


Figure 1: System architecture.

the functions of the point transfer system. To verify the above ideas, we use simulations to validate and evaluate the technical performance of the system. In the end, the practical system should be implemented and tested in field experiments.

3.2. Algorithm for Distributed IoT Devices. The function of a point transfer system is to make point payment available in normal or disaster situations. The point transfer procedure is shown in Figure 1, and the referenced hardware is shown in Figure 2; the user can use a smartphone or a smart device to connect to a node in the point transfer system. When the user chooses to send points from A to B, it sends out a point transfer request to the nodes. The node received the transaction request will broadcast the transaction to the surrounding nodes using its signature. Then, the nodes received the broadcast request will verify the written signature in the packet. If the signature is valid, the node appends its own signature and continues to forward this packet to the next node. When the packet contains enough signatures, this transaction is considered to be true and stored in the ledgers held by the nodes. In LPTS, all the nodes are maintaining the ledger's consistency. This act involves verifying transmission requests. Algorithm 1 shows the verification logic of a transaction in the point transfer function. When a node receives a transaction request from users, it broadcasts this request to the nodes around, with its own verification signature in the message. The nodes receiving the broadcast request will first verify the sender node's signature. The node shall add its own signature to the message once the previous signature is verified and forwards the message to other nodes. When message contains enough number of signatures, this transaction is verified, and the record will be added to the received node's ledger.

Algorithm 1 and Figure 3 describes the process of a transaction request (simulation scenario).

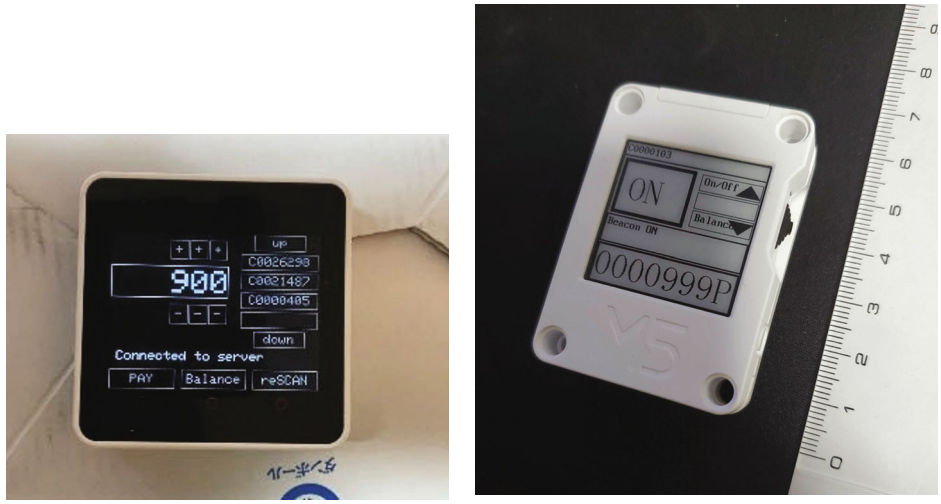
(1) Create N nodes

(2) Create authentication mechanism and forwarding mechanism for each node

(3) Initial a book to keep the transferred points recording, and create initial among of points in the book

(4) Perform point transfer operations according to a random schedule of transaction request

(5) After verifying the transactions, the updated information is written in the ledger book



(a) Payment operation terminal

(b) User device

(c) Nodes

Figure 2: Device examples.

3.3. Evaluation. The first priority to validate the point transfer system is to make sure the system is stable. We need to evaluate the system's robustness, since LPWA network may fail in handling large data transmission for the point transfer management. In the results, we compare it with a bitcoin-like ledger system to see the process time and packet deliver success rate is in the safe zone.

Based on the system architecture in Figure 1, we design an experimental setup that miniaturizes the hardware and uses LPWAN for communication. It is mainly composed of three parts (samples shown in Figure 2): payment operating terminals, user devices, and nodes.

(1) Node. As shown in Figure 4, a node uses Bluetooth module to communicate with smartphones and user devices. The ARM-based computer process all the requests, verification, and packet forwarding. The LPWAN module is used to communicate with other nodes using 920 MHz radio

(2) Payment operation terminal. The payment operation terminal is based on a commercially available microcomputer with integrated BLE module to communicate with the distributed ledger nodes

(3) User device. We built a prototype private key device using a low energy BLE integrated microcomputer to store account IDs and encryption keys. It can communicate with smartphones to send encrypted account IDs or with nodes to check balances

In Figure 5(a), we can see the success rate results with various conditions. With the options in the simulation, we can change the value of packet data error ratio and packet loss ratio. The packet data error ratio is the possibility of data error happening while delivering the data packet. The packet loss ratio is the rate of packet loss, also known as timeout in the network's communication. We set up 50 nodes in the simulation and preset the probability of holding appropriate ledger of 100%. With the increase of both packet data error ratio and packet loss ratio, the packet delivery success rate is decreasing gradually. But the system remains highly robust even if the two ratios are at 40%.

In Figure 5(b), we can see the process time comparison between a bitcoin-like system (red dots) and our system (blue dots). When the number of node is less than 50, the process time of our system is lower. This means our system is suitable to deploy in small scale of nodes in limited areas.

InitializeM; //The number of nodes
InitializeL[]; //The ledger
InitializeB[0 ⋯ *M*] //The candidates of received node *j*'s update block
Data:*T*, *total_node*, *wait_time*
Result:*request_count*, *new_segment_count*, *success_rate*
function transaction_request(*T*)
Receive requested transaction *T* from the points transfer terminal;
if*T* is not *NULL***then**
my_nodeID ⟵ *host*
Send *T* to other nodes;
else
my_nodeID ⟵ *guest*
Receive *T* from other nodes;
end
if*T* is not *NULL***then**
X ⟵ *userID* of *point_sender* in *T*;
Y ⟵ *userID* of *point_receiver* in *T*;
Calculate candidates of new balances P_x and P_y based on blocks in $L[0 \cdots n]$;
my_nodeID ⟵ ″*X* ⟵ P_x″ and ″*Y* ⟵ P_y″
for*i* = 1**to***M***do**
if*wait_time* ≤ *threshold***then**
Receive *B*[*i*] as calculated candidate of new balances from other nodes;
end
end
Calculate B_u as a majority vote of $B[0 \cdots M]$;
Send approval results to the points transfer terminal;
n ⟵ *n* + 1;
L[*n*] ⟵ $B_u p$;
end

Algorithm 1: Point transfer function

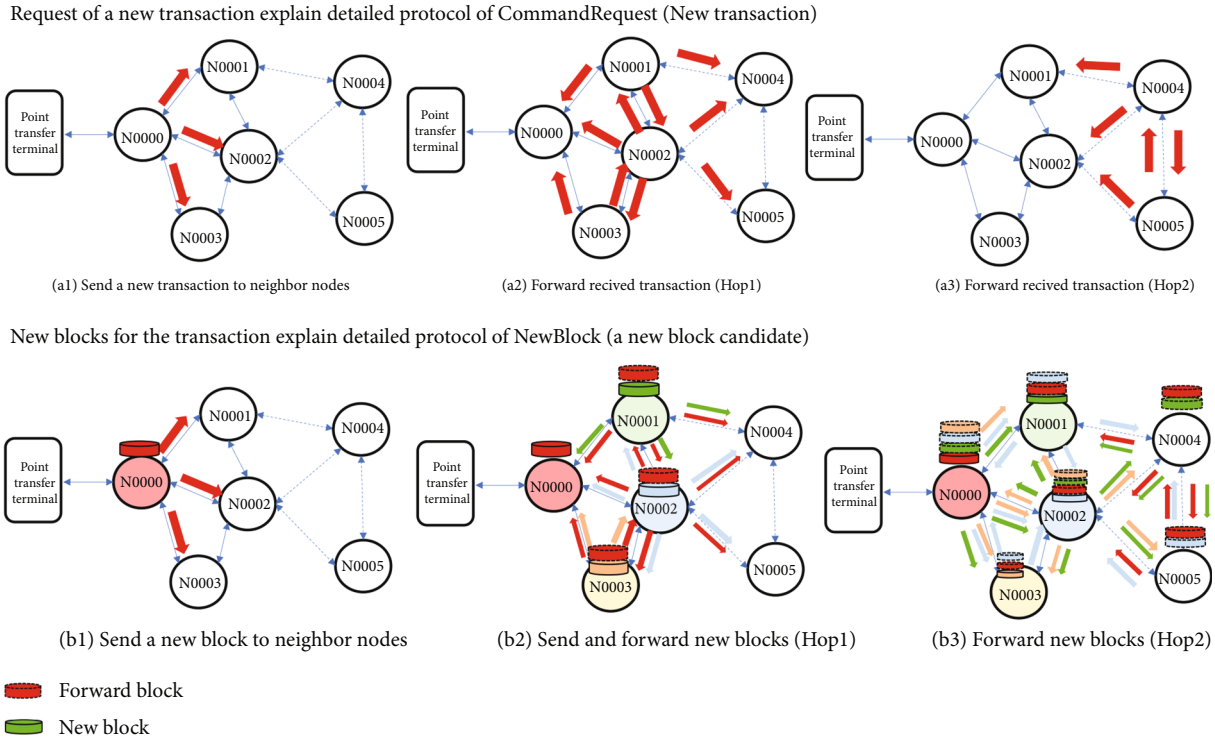


Figure 3: Ledger operation [29].

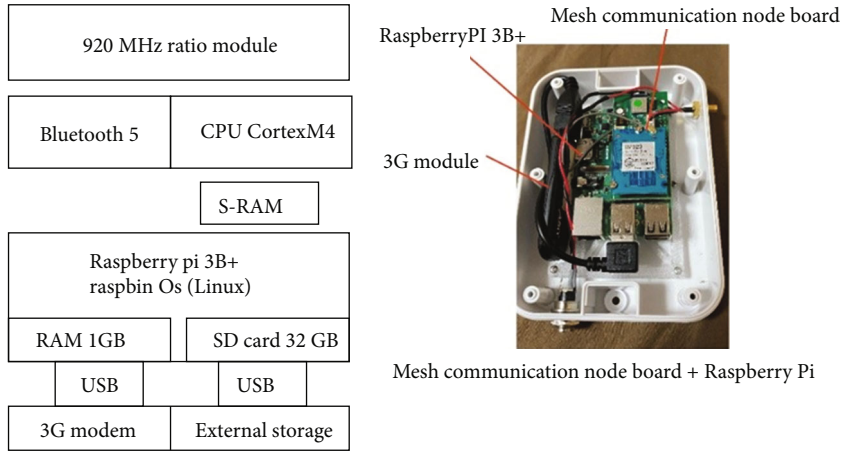
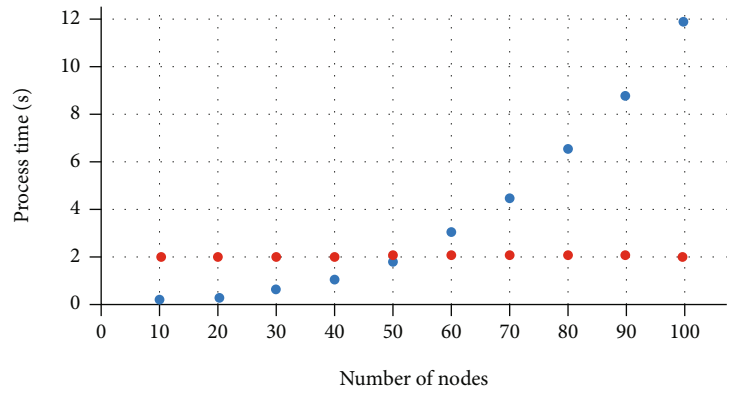


Figure 4: Node configuration.

Packet data error ratio \ Packet loss ratio	0%	20%	40%	60%	80%
0%	100.0%	100.0%	100.0%	100.0%	100.0%
10%	100.0%	100.0%	100.0%	100.0%	93.5%
20%	100.0%	100.0%	100.0%	100.0%	93.9%
30%	100.0%	100.0%	100.0%	100.0%	77.1%
40%	100.0%	100.0%	100.0%	98.0%	64.4%
50%	100.0%	100.0%	96.0%	90.0%	35.6%
60%	100.0%	96.0%	88.0%	84.0%	20.0%
70%	96.0%	86.0%	82.0%	60.0%	22.2%
80%	60.0%	44.0%	42.0%	20.0%	9.1%
90%	20.0%	20.0%	24.0%	4.0%	6.8%

(a) Success rate with various conditions



(b) Process time of bitcoin-like system (red dots) and our system (blue dots)

Figure 5: Success rate and process time compare.

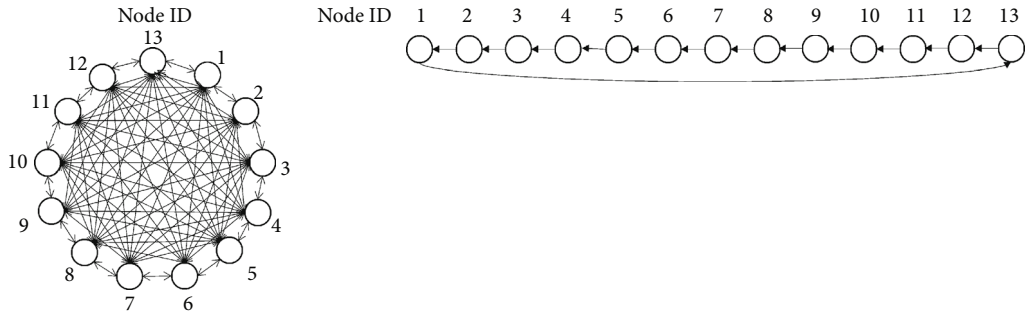
Table 2: Node specification.

Items	Specification
Processor of node	Raspberry-Pi Cortex-A53 (ARMv8) 64-bit Soc@1.4 GHz 1 GB RAM
Communication distance (high-speed mode)	Maximum 400 m Typical 100 m
Communication speed (high-speed mode)	Maximum 50 kbps Typical 10 kbps

4. Implementation of Ledger-Based Points Transfer System for Small-Scale IoT Devices in LPWAN

4.1. System Design and Prototype. To realize a LPWA-based ledger system in IoT devices, we need to face and solve several problems. First, the LPWA network and Raspberry-Pi devices form a limited platform with low bandwidth network and low processing capability. The operating system and daemon software need to be compact and simplified.

Figure 4(a) shows the topology of the modules in a node, and Figure 5(b) shows the prototype of a nod device. Table 2 shows the specification of the prototype. The main board in the node is an ARM-based small computer, Raspberry-Pi. It has 1 GB RAM and a Cortex-A53 SoC. In the communication module part, the Bluetooth module talks to the terminals and user devices so they can display the balance and operate the point transfer system. 3G module is not used in this part, but it shows the ability to communicate via cellular network. LPWAN module is used to build the mesh network among the



(a) Mesh topology

(b) Chain topology

Figure 6: Experiment topology.

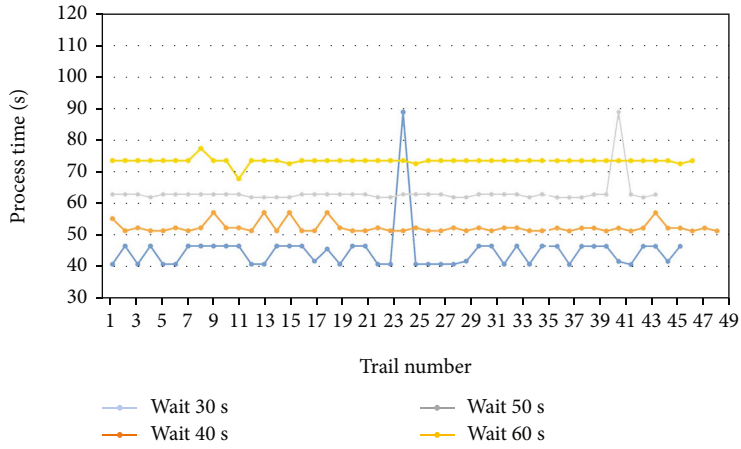


Figure 7: Process time result of small scale experiment.

nodes. It can provide wireless connection range up to 400 m and speed in high speed mode up to 50 kbps. We set the communication speed to 50 kbps to maximize the bandwidth.

4.2. Evaluation. We use the prototype nodes (Figure 4) to build the experiment topology. The LPWAN can broadcast one-to-many communications; however, we set up the system to limit the nodes that can receive messages from one node. In the experiment, there are two kinds of topology that applied to the nodes. In Figures 6(a) and 6(b), (a) shows the nodes can communicate with each other without limitation via LPWAN, and (b) shows a preset node topology that limits the packet delivery direction and path among the nodes. In the small-scale experiment, we use 13 nodes, same number as the multihop nodes used in large scale experiment. The small-scale experiment is for evaluating the efficiency of large-scale system. We suppose the system handle 40 nodes in the community area where one node will send messages to an average of 3 nodes in one transmission. This configuration will cause 13 multihopping (forwarding) to keep same messages for every node.

The evaluation measures process time for the point transfer system in the following steps.

(1) Send a transaction request ("send A to C 100 pts") to one contact node

(2) Forward the requests to other nodes

(3) The message will be broadcast to all nodes via multihop nodes in LPWAN

(4) Create an additional new block in each node

(5) Each node sends the new block data to other nodes

(6) Each node receives the new block data from other nodes

(7) Each node decides the new block data by majority voting of data from other nodes

(8) Append the new block to the ledger

(9) Return the transaction results and answer the latest balances of A and C

In each node, there is a parameter called "wait time." It is between steps 2 and 4 to confirm if the communication succeeded with other nodes. The process time results depend on the "wait time." Figure 7 shows the total process time for 44 to 49 trails, with different "wait time." For example, if "wait

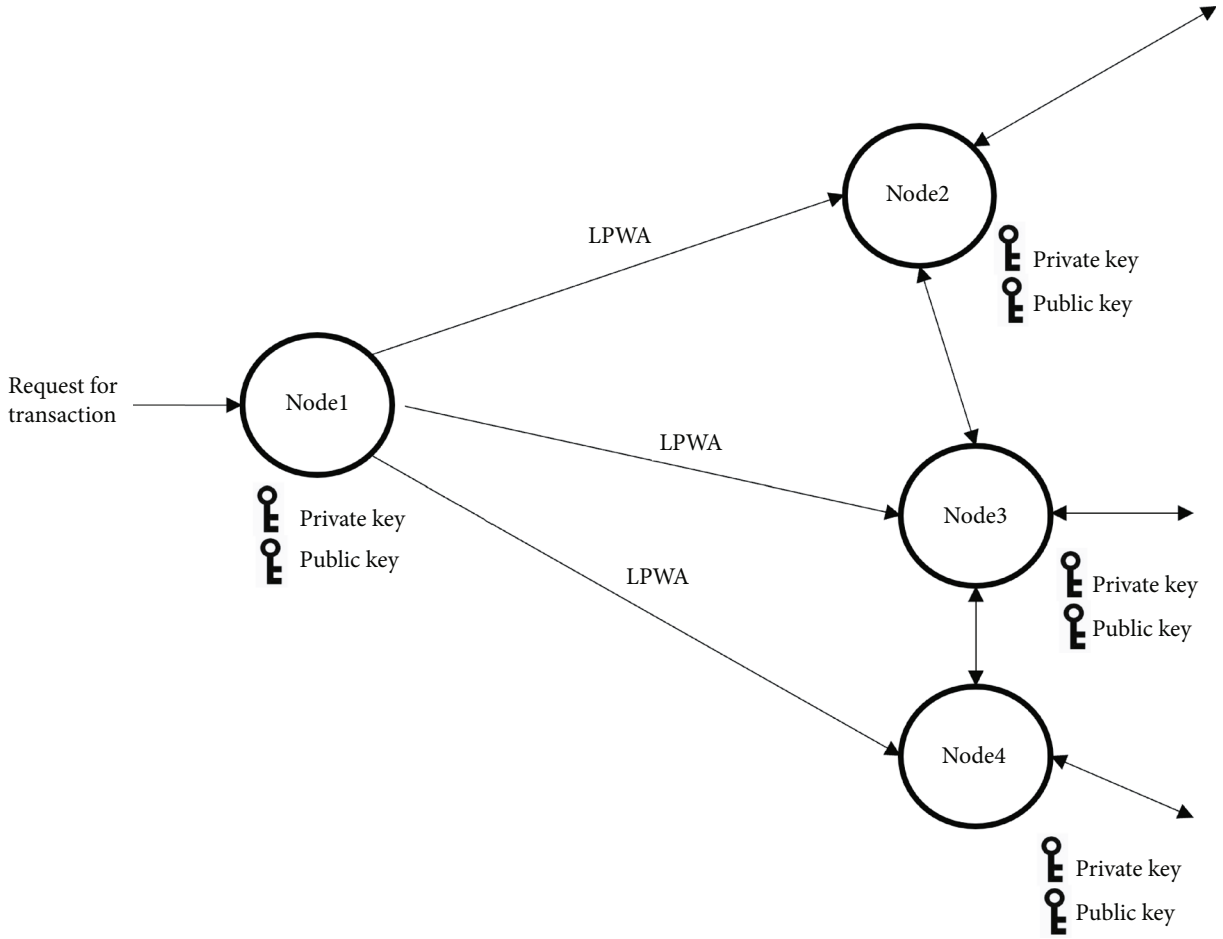


Figure 8: Message delivery with signature.

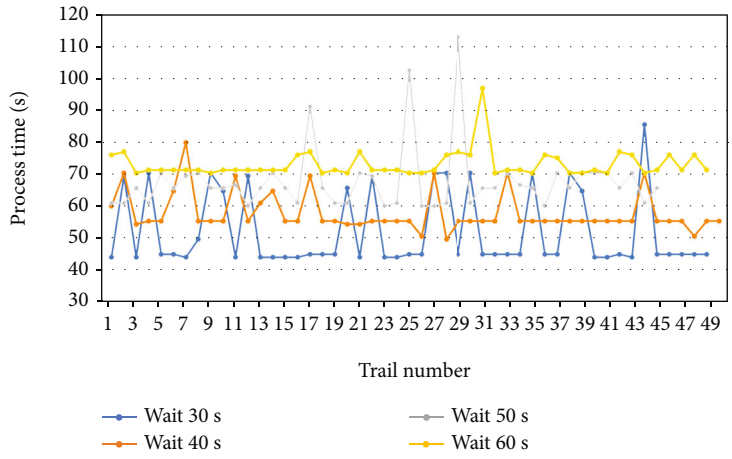


Figure 9: Process time result with signature.

time" is 30 s, one of the trail's process time is about 90 s. This may be caused by communication congestion due to LPWAN's low bandwidth. Also, we can see that the process time of lower "wait time" tends to have much variation. When "wait time" is at around 40 to 60 seconds, the variation of the process time of a transaction is quite stable, making 40 seconds the top option in selecting "wait time."

5. Extension of Ledger-Based Points Transfer System for IoT Devices in LPWAN

After designing LPTS and building its prototype, we have found some optional optimizations that might benefit the system. The extension of LPTS includes additional security option, packet transmission optimization, and system's

InitializeM; //The number of nodes
InitializeL[]; //The ledger
InitializeB[0 ⋯ *M*]; //The candidates of received node *j*'s update block
InitializeS[]; //Selected nodes
Data: *T*, *total_node*, *wait_time*
Result: *request_count*, *new_segment_count*, *success_rate*
function *transaction_request*(*T*);
Receive requested transaction *T* from the points transfer terminal;
if *T* is not *NULL* **then**
  my_nodeID ⟵ *host*
  Send *T* to other nodes;
else
  my_nodeID ⟵ *guest*;
  Receive *T* from other nodes;
end
if *T* is not *NULL* **then**
  X ⟵ *userID* of *point_sender* in *T*
  Y ⟵ *userID* of *point_receiver* in *T*
  Calculate candidates of new balances P_x and P_y based on blocks in $L[0 \cdots n]$;
  my_nodeID ⟵ ″*X* ⟵ P_x″ and ″*Y* ⟵ P_y″
  for *i* = 1 **to** *M* **do**
    if *wait_time* ≤ *threshold* **then**
      Receive *B*[*i*] as calculated candidate of new balances from other nodes;
    end
  end
  if *my_nodeID* not in *S*[] **then**
    for *i* = 1 **to** *M* and *B*[*i*] not received **do**
      Forward *B*[*i*];
    end
  end
  Calculate B_u as a majority vote of $B[0 \cdots M]$;
  Send approval results to the points transfer terminal;
  n ⟵ *n* + 1
  L[*n*] ⟵ $B_u p$
end

Algorithm 2: Optimized transaction request function

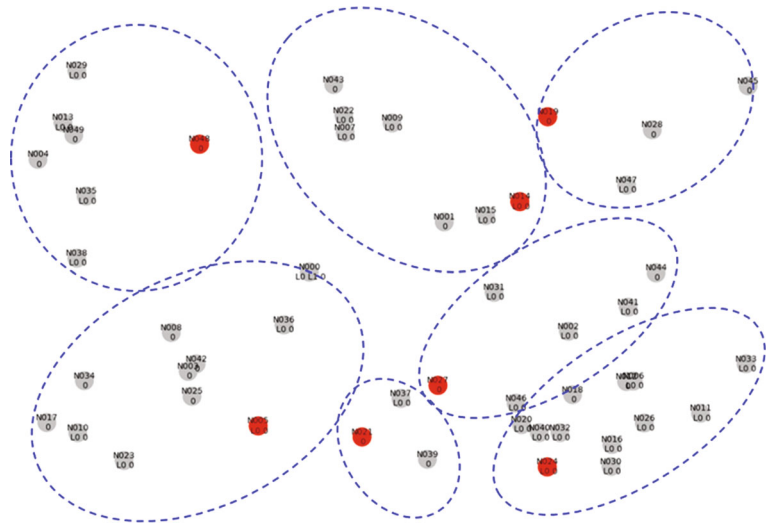
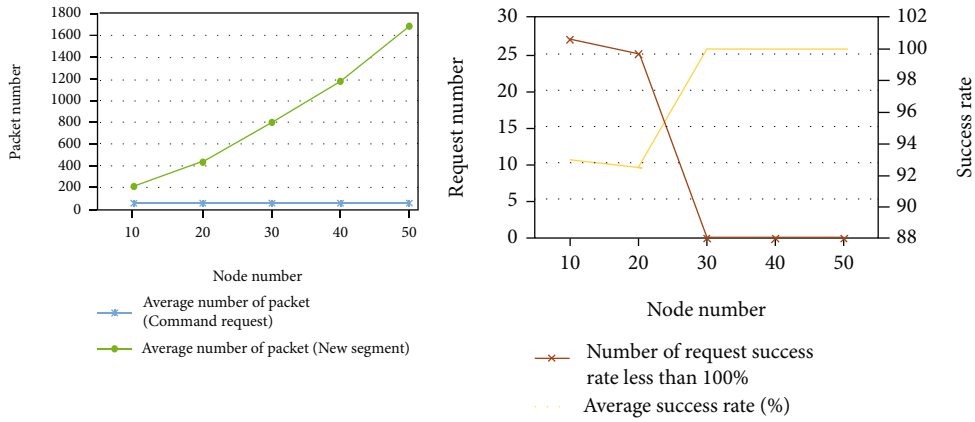


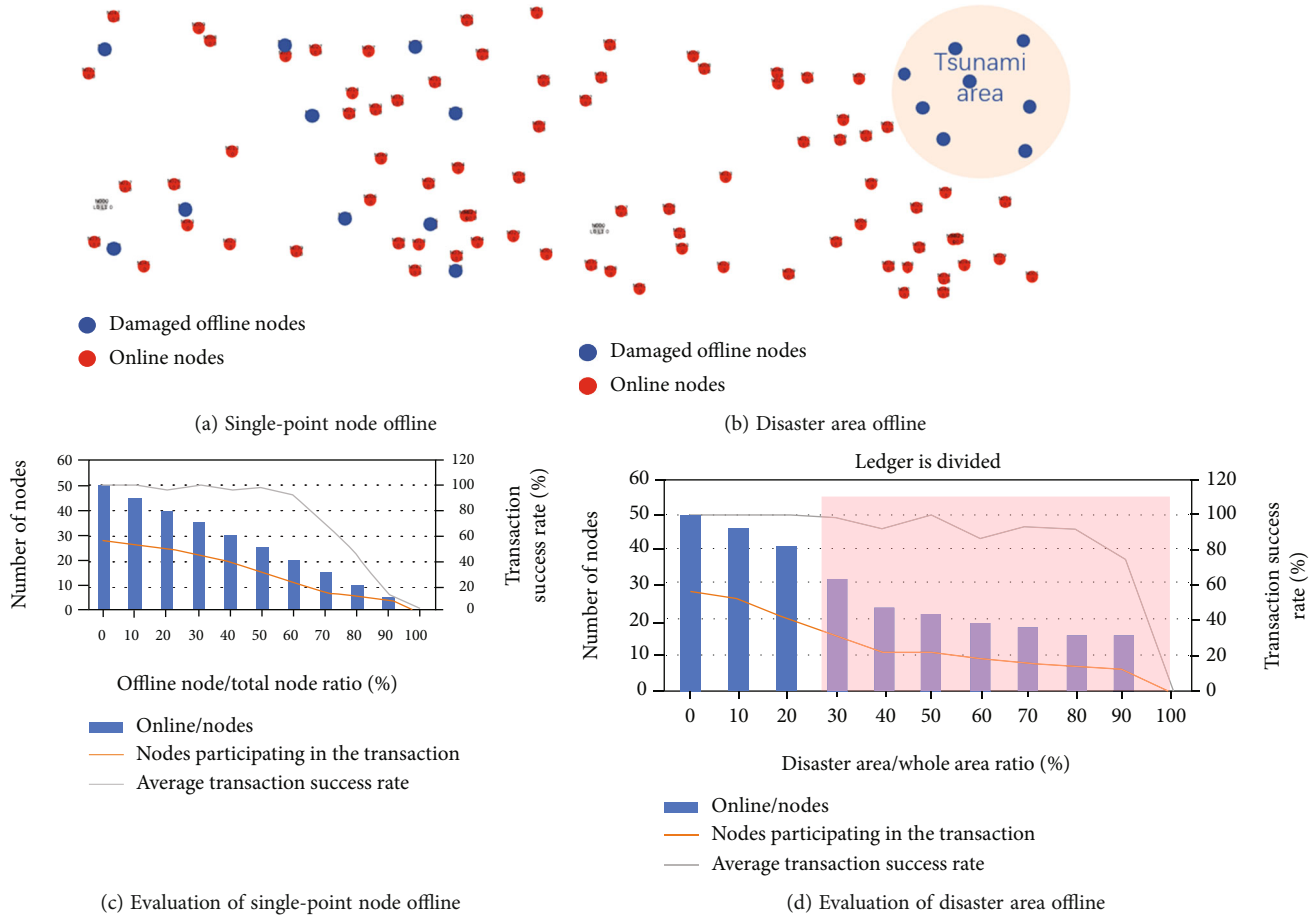
Figure 10: *K*-means clustering example.



(a) Generated packet number compare

(b) Success rate and insecure requests

Figure 11: Packet reduction results.



(a) Single-point node offline

(b) Disaster area offline

(c) Evaluation of single-point node offline

(d) Evaluation of disaster area offline

Figure 12: Disaster scenario evaluation results.

disaster tolerance. The security enhancement option is based on LPTS prototype and evaluated in experiments. The packet transmission optimization and disaster tolerance are evaluated in simulations.

We aim to validate and evaluate the proposed point transfer system and its performance in the simulated environment. By using a Python language-powered simulator, we manage to evaluate the proposed system's performance. This part involves packet success rate under different communication error and loss rate, packet success rate with different k value in optimization, and packet success under disaster scenario.

5.1. Additional Signature for Higher Security. In addition to the nonsignature-based system we tested above, we have also tested a higher security method by adding ECDSA (FIPS

186-3 Digital Signature Standard)-based signatures to the messages. With signature, data packet size is 198 bytes, 134 bytes longer than the 64 bytes nonsignature messages. Figure 8 shows the message delivery processes with signatures added to the messages. We added signature to the following steps:

(1) Transaction requests

(2) New block data (candidates)

Figure 9 shows the process time of the trails in the similar conditions of the above part. We can see that with signature, the process time becomes longer and has wide variations due to larger packet size and LPWAN's limitation. The process finishes within 120 s without errors. The overall ledger management is still intact.

5.2. Function to Optimizing Packet Transmission. By using LPWAN-based communication environment, the bandwidth for the ledger system is limited. According to the simulation of the system, without considering the bandwidth limit, the network needs to handle 1742 packets by generate one transaction. The overall packet size hits about 900 kbit, and with the bandwidth limit of LPWAN which is 50 kbps, it needs about 15 min to complete one transaction. An optimal algorithm is needed to make the system finish one transaction faster and remain tamper-proof.

To reduce overall data size, we choose to reduce transmission packet numbers by reducing number of nodes that can forward the packets. We select a number of nodes from all the nodes to offer multihop function to forward packets. All nodes are divided into several clusters to make sure that most of the nodes can join the verification of the transaction request. As shown in Algorithm 2 and Figure 10, we use K -means clustering [30] with a preset k, to select multihop nodes. First, we create N nonmultihop nodes (all the nodes). Then, we perform K-means clustering with the location information of each node and select the nodes closest to the output location information to be the multihop nodes (red marked nodes). Finally, the selected nodes are given multihop function to finish preparing the system before running. Because the LPWA network operates in a low bandwidth mode, it is necessary to find a way to further reduce the data traffic in the network. We use K-means clustering algorithm to find center node of each cluster in the whole area. This chosen node is capable of multihopping that can receive and send multiple packets at the same time. The simulator can generate random nodes in a certain area with preset node numbers. Each node has LPWA communication ability to simulate data traffic in the network. In the simulation, we use different sets of multihop node numbers k to cluster all the nodes. By increasing number k, we can evaluate from nonmultihop to fully multihop scenarios. This gives us concepts in different scales to see the best balance between overall system stability and network data traffic consumption.

In Figure 11, the two result figures are oriented by k value from small to large. CommandRequests stands for transaction request packet number, and NewSegment stands for transaction packet number generated by transaction requests. In (a), the average number of CommandRequests is at the same level, and the number of NewSegment is from smallest to largest, which means that changing the number of multihop function nodes does not change the number of transaction requests, but affects the overall packets of new blocks for the transaction. Therefore, it is effective reducing the number of multihop function nodes to reduce the overall communication traffic. In (b), at the same time, the average update success rate of new blocks is not 100%, which leads to a reduction in the overall security and integrity of the network. We cannot blindly reduce the k value to reduce the traffic volume. In this simulation, reducing multihop node number to 30, in a 50 overall node number, is a balanced result.

5.3. Function to against Disaster. According to the design principle of our proposed system. The nodes consume small amount of power and can keep running for a long period of time on battery powers to avoid power shortage. However, there are some inevitable disasters like earthquake and tsunami that can disable or destroy the structure of certain area, meaning the nodes in that area will be offline. In that sense, putting the distributed ledger system in disaster scenarios is important to evaluate its robustness. The communication principle should remain the same with Algorithm 1, and the transaction success rate is the result showing the system robustness.

When it comes to disaster scenarios, we categorize them into two kinds, single-point node offline and disaster area offline. Figures 12(a) and 12(b) show the node topology of the two kinds of disasters. In single-point node offline, the offline nodes will take place in the whole area evenly. In disaster area offline, nodes inside the disaster area will be offline. Figures 12(c) and 12(d) show the results of the two kinds of disaster scenarios. In single-point node offline, with the online nodes decrease gradually, and the nodes participating in the transaction decrease. But the success rate remains at a high level under the online node number which is less half of the overall node number. The same situation happens in the disaster area offline scenario, but we have noticed that when more than 30% of the nodes are offline, the ledger is actually divided into two or more. This means the ledger system is no longer whole, and it leads to security issue. In the tsunami scenario shown in Figure 12(b), the failure area is set to the upper right corner because the ocean region is located at the edge of the installation area. On the other hand, in a volcanic eruption scenario, the failure could occur in other locations like the center of the area. A failure in the center of the area increases the probability that the communication area will be divided into two or more parts. The same situation can be seen in Figures 12(c) and 12(d), as more than 30% of the failures result the area divided. Therefore, it is concerned that the percentage of the failure area is more dominant than the location of the failure area.

6. Conclusion

Point transfer system merging with LPWAN communication technology provide us a new way to make use of small IoT platforms. LPWAN provides low-power and wide-area radio communication network to realize end-to-end connection. Third-party points transfer system can now overcome

disasters to become a financial solution and application in local areas. The decentralized design principle of our proposed system solves the traditional centralized system issues like asset data tampering and low robustness. We also proposed an optimal solution to reduce packet congestion in LPWAN and tested it and disaster scenario robustness in simulations. At last, we implemented the system in small-scale IoT devices and made experiment to prove our design which is valid and robust.

Data Availability

Access to data is restricted. The data used in this paper is collected in experiment in the field and may contain public information. Researchers can contact the authors for the access to the data.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Authors' Contributions

Xin Qi is responsible for the conceptualization, methodology, software, experiment, and writing—draft preparation, reviewing, and editing; Keping Yu for the conceptualization, methodology, and writing—draft preparation; Toshio Sato for the conceptualization, data curation, and writing—reviewing; Kouichi Shibata and Isao Konno for the software and validation; Takanori Tokutake, Rikiya Eguchi, and Yusuke Maruyama for the software and experiment; Zheng Wen for the experiment and data curation; Kazuhiko Tamesue and Yutaka Katsuyama for the writing—reviewing and editing; and Kazue Sako and Takuro Sato for the conceptualization and writing—reviewing.

Acknowledgments

This research and development work was supported by the MIC/SCOPE 205003002, "Certification System Using Simplified LPWA-Based Distributed Ledger Technology."

References

[1] H. Pirayesh, P. Kheirkhah Sangdeh, and H. Zeng, "Securing ZigBee communications against constant jamming attack using neural network," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4957–4968, 2021.

[2] U. Raza, P. Kulkarni, and M. Sooriyabandara, "Low power wide area networks: an overview," 2016, http://arxiv.org/abs/1606.07360.

[3] K. Yu, K. Shibata, T. Tokutake et al., "A lightweight ledger-based points transfer system for application-oriented LPWAN," in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, pp. 1972–1978, Chengdu, China, December 2020.

[4] S. Rasveen, K. C. Agrawal, and S. Kumar, "Coverage and latency analysis for NB-IoT in uplink transmission," in *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, pp. 330–334, Chiangrai, Thailand, March 2022.

[5] Y. Chen, Y. A. Sambo, O. Onireti, and M. A. Imran, "A survey on LPWAN-5G integration: main challenges and potential solutions," *IEEE Access*, vol. 10, pp. 32132–32149, 2022.

[6] P. Chaudhari, A. K. Tiwari, S. Pattewar, and S. N. Shelke, "Smart infrastructure monitoring using LoRaWAN technology," in *2021 International Conference on System, Computation, Automation and Networking (ICSCAN)*, pp. 1–6, Puducherry, India, July 2021.

[7] H. E. Elbsir, M. Kassab, S. Bhiri, and M. H. Bedoui, "Evaluation of LoRaWAN class b efficiency for downlink traffic," in *2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 105–110, Thessaloniki, Greece, October 2020.

[8] A. Lavric, A. I. Petrariu, and L. Anchidin, "Internet of things software defined radio technology for LoRaWAN wireless communication: a survey," in *2021 12th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, pp. 1–4, Bucharest, Romania, March 2021.

[9] S. Aguilar, D. S. W. La-Torre, A. Platis et al., "Packet fragmentation over Sigfox: implementation and performance evaluation of SCHC ACK-on-error," *IEEE Internet of Things Journal*, vol. 9, no. 13, pp. 11057–11070, 2021.

[10] A. I. Petrariu and A. Lavric, "Sigfox wireless communication enhancement for internet of things: a study," in *2021 12th International Symposium on Advanced Topics in Electrical Engineering (ATEE)*, pp. 1–4, Bucharest, Romania, March 2021.

[11] A. A. F. Purnama and M. I. Nashiruddin, "Sigfox-based internet of things network planning for advanced metering infrastructure services in urban scenario," in *2020 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communications Technology (IAICT)*, pp. 15–20, Bali, Indonesia, July 2020.

[12] Y. Lalle, L. C. Fourati, M. Fourati, and J. P. Barraca, "A comparative study of LORAWAN, Sigfox, and NB-IoT for smart water grid," in *2019 Global Information Infrastructure and Networking Symposium (GIIS)*, pp. 1–6, Paris, France, December 2019.

[13] R. Banno and K. Shudo, "Simulating a blockchain network with simblock," in *2019 IEEE international conference on blockchain and cryptocurrency (ICBC)*, pp. 3-4, Seoul, Korea (South), May 2019.

[14] H. Yu, M. H. Cheung, L. Gao, and J. Huang, "Public Wi-Fi monetization via advertising," *IEEE/ACM Transactions on Networking*, vol. 25, no. 4, pp. 2110–2121, 2017.

[15] F. Farha, H. Ning, S. Yang, J. Xu, W. Zhang, and K.-K. R. Choo, "Timestamp scheme to mitigate replay attacks in secure ZigBee networks," *IEEE Transactions on Mobile Computing*, vol. 21, no. 1, pp. 342–351, 2022.

[16] Z. Wang, Y. Cao, L. Kong et al., "Reference waveforms forward concurrent transmissions in ZigBee communications," *IEEE/ACM Transactions on Networking*, vol. 28, no. 4, pp. 1629–1642, 2020.

[17] M. Chen, Y. Miao, Y. Hao, and K. Hwang, "Narrow band internet of things," *IEEE Access*, vol. 5, pp. 20557–20577, 2017.

[18] E.-H. Kim, K. Lee, T.-J. Park, and H.-W. Son, "Unlicensed-band single-hop lpwa repeater for smart-city iot applications," in *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 446–448, Jeju Island, Korea, October 2021.

[19] E. Harinda, S. Hosseinzadeh, H. Larijani, and R. M. Gibson, "Comparative performance analysis of empirical propagation models for lorawan 868mhz in an urban scenario," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, pp. 154–159, Limerick, Ireland, April 2019.

[20] R. Teng, K. Yano, and Y. Suzuki, "Estimation of network type based on the response delay property," in *2022 24th International Conference on Advanced Communication Technology (ICACT)*, pp. 1–6, PyeongChang Kwangwoon_Do, Korea, February 2022.

[21] S. Kang, J. Eom, J. Eom, and S.-I. Kang, "Time synchronization method for LPWA using simple sync procedure in IoT wireless network," in *2020 International Conference on Information and Communication Technology Convergence (ICTC)*, pp. 1851–1854, Jeju, Korea, October 2020.

[22] K. Yu, Z. Guo, Y. Shen, W. Wang, J. C.-W. Lin, and T. Sato, "Secure artificial intelligence of things for implicit group recommendations," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 2698–2707, 2021.

[23] Q. Zou, G. Li, and W. Yu, "An integrated disaster rapid cloud service platform using remote sensing data," in *2017 IEEE International Geoscience and Remote Sensing Symposium (IGARSS)*, pp. 5221–5224, Fort Worth, TX, USA, July 2017.

[24] P. R. Nair and D. R. Dorai, "Evaluation of performance and security of proof of work and proof of stake using blockchain," in *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, pp. 279–283, Tirunelveli, India, February 2021.

[25] X. Yang, Y. Chen, and X. Chen, "Effective scheme against 51% attack on proof-of-work blockchain with history weighted information," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 261–265, Atlanta, GA, USA, July 2019.

[26] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green internet of things," *ACM Transactions on Internet Technology (TOIT)*, vol. 21, no. 3, pp. 1–20, 2021.

[27] N. Shi, L. Tan, W. Li, X. Qi, and K. Yu, "A blockchain-empowered AAA scheme in the large-scale HetNet," *Digital Communications and Networks*, vol. 7, no. 3, pp. 308–316, 2021.

[28] S. S. Panda, B. K. Mohanta, M. R. Dey, U. Satapathy, and D. Jena, "Distributed ledger technology for securing IoT," in *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–6, Kharagpur, India, July 2020.

[29] X. Qi, K. Yu, T. Sato et al., "Optimizing packet transmission for ledger-based points transfer system in LPWAN: solutions, evaluation and standardization," in *2021 ITU Kaleidoscope: Connecting Physical and Virtual Worlds (ITU K)*, pp. 1–8, Geneva, Switzerland, December 2021.

[30] P. Sasikumar and S. Khara, "K-means clustering in wireless sensor networks," in *2012 Fourth international conference on computational intelligence and communication networks*, pp. 140–144, Mathura, India, November 2012.