IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 18 December 2022, accepted 26 January 2023, date of publication 31 January 2023, date of current version 6 February 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3241104

RESEARCH ARTICLE

Proposal for Low-Layer Metadata Collection Technology to Enhance IoT Metadata Utilization

RYOTA SHIINA, (Member, IEEE), SHINYA TAMAKI, CHE HUANG, TOMOYA HATANO, TAKASHI YAMADA, TATSUYA SHIMADA, AND TOMOHIRO TANIGUCHI

NTT Access Network Service Systems Laboratories, NTT Corporation, Musashino 180-8585, Japan

Corresponding author: Ryota Shiina (shiina.ryota@ieee.org)

ABSTRACT With the rapid spread of Internet of Things (IoT) services, the number of sensor devices has exploded, and the complexity of managing sensor devices has become a problem. To solve this problem, a metadata-based approach that uses the unique environmental information associated with each device for its management is being developed. This paper focuses on metadata collection for device management and control, and proposes a new collection method that uses low-layer communication while not modifying the existing protocol. Our proposal utilizes the extended area of the probe request (PRQ) frame of IEEE 802.11, which is a layer-2 protocol, to collect metadata. This makes it possible to achieve stable operation even on inexpensive and resource-limited IoT devices, and to realize metadata collection with low communication overhead and power consumption. It is shown to reduce the load on the central processing unit (CPU) and reduce power consumption compared to Internet Protocol (IP) -based metadata collection (layer-3 protocol and above). In addition, in terms of time sensitivity, the collection delay at the time of rising from deep sleep is reduced by 89.8% compared to IP-based techniques. Furthermore, as a benefit of low-layer collection, it enables periodic metadata collection in the background regardless of network connection above the IP layer. To demonstrate this benefit, an example of applying metadata collection to device management is prototyped and its feasibility is experimentally confirmed.

INDEX TERMS IoT, metadata, low-layer metadata collection, wireless local area network.

I. INTRODUCTION

The Internet of Things (IoT) involves the collection of large amounts of data by a huge number of sensors [1], [2]. Recently, the price of sensors has been reduced, and cheap and simple sensors are increasing in the market. As a result, the IoT market is expanding explosively [3], [4]. The market expansion is expected to continue into the future. Unfortunately, as the number of sensors increases, the problem of complicated sensor management will worsen. In data management to guarantee the reliability of collected data, the conventional approach is to detect events from the target sensing data itself [5], [6], [7]. However, the increasing complexity of data management in recent years has exposed the need for more detailed information. Therefore, utilizing metadata for data management is considered to be a promising new approach [8], [9], [10]. Metadata is data associated with devices that acquire sensor data and is defined as device-specific information [8], [11]. (e.g.: device location, installer, installation date/time, device serial number) These metadata can be collected and utilized to aid in more detailed sensor data management. As a result, it is expected to improve the reliability of sensor data.

A conceptual architecture for applying metadata to data management is shown in Figure 1. In this architecture, metadata about the IoT device is collected via the network in addition to the sensing data normally collected by the IoT device. The collected metadata is stored together with the sensing data, and the metadata is used to manage the IoT device and the sensing data itself. For example, there are several studies on metadata-based device and data management. Reference [12] proposes a conceptual metadata utilization model to abstract the collected sensor data. Sensor data and metadata are merged and used for sensor management.

The associate editor coordinating the review of this manuscript and approving it for publication was Byung-Seo Kim.

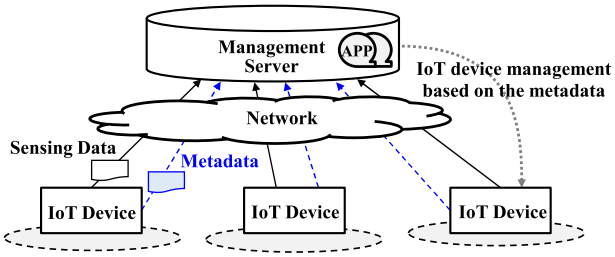

FIGURE 1. Conceptual architecture for applying metadata to management.

In addition, [13] clearly presents the types of metadata to be collected, and describes the management of linking sensing data and metadata.

While such metadata-based integrated management techniques can be enhanced by handling a wide variety of metadata, there are challenges in how to handle the extremely large quantities of metadata expected. In order to reduce the overall cost of IoT systems, metadata collection must be able to collect more metadata with less power consumption. Also, from a computing resource perspective, it is necessary to be able to collect more data and metadata from less expensive IoT devices. Furthermore, from the perspective of IoT device and data management, the main data and metadata collection network layers must be separated. In conventional collection approaches, data and metadata are basically collected using the same method and on the same network layer, which creates limitations in metadata utilization. (e.g. it depends on the network connection for the main data collection, making it difficult to utilize metadata in situations such as initial network connection of IoT devices).

Therefore, in this paper, we propose a novel layer-2 metadata collection scheme to achieve metadata collection with lower power consumption and lower computational resources compared to previous collection methods that utilize protocol stacks above IP. Focusing on Wireless Local Area Network (WLAN) systems, the proposal transfers the collected metadata in the Probe Requests (PRQs) used for negotiation. This enables collection in the layer-2 of existing protocols and enables metadata collection with lower power consumption and fewer computational resources. In addition, it enables the separation of data and metadata collection layers and flexible metadata utilization for network management. We implement a prototype and quantitatively evaluate the underlying performance in terms of power consumption, computing resources and network delay to demonstrate the proposal's effectiveness. Using a prototype, we also quantitatively evaluate the latency of metadata collection. Furthermore, we build a system that applies our proposal to network management and qualitatively demonstrate the benefits of IP independence.

Our contributions in this paper can be summarized as follows.

- A layer-2 metadata collection scheme based on the existing 802.11 negotiation protocol is proposed and prototyped.
- The proposal is implemented on actual IoT devices and quantitatively evaluated in terms of power consumption, computing resources, and latency compared to metadata collection with the IP-based approach.
- A management system applying the proposal to network management is built, and its qualitative benefits are presented in terms of IP-independence of metadata collection, which is one of the features of the proposal.

Section II describes related works of our study. Section III describes the entire proposal. First, we will discuss the architectural details and configuration of the low layer metadata collection scheme. We also show the advantages of the proposal. Section IV describes implementation of the proposal. Section V describes the results of evaluation to confirm some of the advantages of the proposal. Finally, Section VI summarizes the paper.

II. RELATED WORKS

Our study is related to schemes that collect metadata and use it to manage IoT devices and sensing data. There have been various important studies on the use of metadata for the management of IoT devices and their sensing data.

In addition to sensing data, a variety of metadata about the IoT devices needs to be collected, therefore the amount of data to be uploaded will be drastically increased. Effective architectures have been proposed in terms of mass data processing for data storage. In [37], [38], and [42], it is shown that distributed processing architectures are effective in terms of processing energy and processing latency.

There are also proposals for metadata storage formats and application programming interface (API) definitions [14], [17], [39], [42]. For example, in [14], it is proposed to convert metadata into context and use both in an integrated manner. An example of converting metadata into context is shown in detail. Also, [17] defines a metadata API for an IoT device management system.

Some frameworks have been proposed to manage sensing data in association with metadata [15], [43]. An integrated framework that combines or abstracts heterogeneous sensing data sources for various applications based on metadata has been described.

There is also a lot of research being done on using metadata to ensure the security, reliability, and privacy of IoT systems [16], [38], [40], [41]. To ensure stronger security, [16], [38], [40] propose the use of blockchain as a way to combine and store collected sensing data and metadata, taking advantage of blockchain's features to achieve highly secure and robust management of IoT systems.

The important references above mention architecture, formats for storing and reading collected data / metadata, APIs, management frameworks, security, etc. However, few studies focus on the metadata collection method itself.

In a normal implementation, metadata will be collected in the same way as the main data. However, when metadata is collected using the same communication protocol as the main sensing data, it is assumed that a communication connection

has already been established, so metadata cannot be used to assign IP addresses or grant connection permissions according to the installation location, which limits its use in device management. Thus, metadata must be collected even before the IP connection is established using a different method (network device, protocol, network layer, etc.) from the main data [18]. In addition, if metadata is to be processed at the same application layer as the main data in IoT devices, the increase in the type and amount of metadata handled will directly lead to an increase in terminal load. Many IoT devices have limited resources and must be implemented as inexpensively as possible.

Therefore, this study proposes a method of collecting metadata on a different network layer from the main data, with lower overheads. In other words, this study differs from other related studies in the following points.

- We establish a low load method for collecting IoT metadata that is independent of the communication connection of the main data.
- The proposed method minimizes the increase in power consumption and computing resources for metadata collection so that a wide variety of metadata can be collected from resource-sparse IoT devices.

This research complements all the important previous studies mentioned above.

III. PROPOSAL

A. LOW-LAYER METADATA COLLECTION

The basic approach of our proposal is to utilize a layer-2 protocol to effect metadata transfer. In particular, we focus on IEEE 802.11, one of the wireless communication methods of the IoT protocol [19]. With the widespread use of IEEE 802.11 communication modules, module costs have been significantly reduced, and various IoT devices now incorporate IEEE 802.11 compliant communication modules [20], [21]. In addition, since the data rate of IEEE 802.11 is higher than that of other IoT wireless systems, it is possible to handle a wide range of data, from small data such as physical sensors to large-capacity data such as high-definition video. Therefore, in our proposal, metadata is collected using layer-2 PRQ in the IEEE 802.11 protocol. This means that low-layer metadata collection can be achieved without changing the IEEE 802.11 protocol.

Figure 2 shows the proposed layer-2 based metadata collection scheme. Its basic configuration consists of an IoT device with a sensor module, gateway, and management server. The management server manages the collected data, IoT devices and network devices. As a premise, the IoT device with sensor module periodically sends the main sensing data to the gateway via IEEE 802.11 for collection by the management server via the wired / wireless network.

On the other hand, IoT devices collect metadata via an interface (e.g. bluetooth interface) that is different from the IEEE 802.11 interface. The collected metadata is stored in the extended domain of the PRQ frame. The stored metadata is then transferred to the gateway separately from the main sensor data. Fig. 3 shows the structure of the PRQ frame in IEEE 802.11 [19]. The body of the PRQ frame has an extensible vender-specific domain and we use this domain to transfer metadata. The gateway reads the vendor-specific domain of the PRQ frame and extracts the metadata. The IoT device identifier and gateway identifier (i.e. MAC address) associated with the metadata are sent together to the management server.

In actual IoT data collection scenarios, the target data may not be obtained correctly for reasons such as the installation location of the IoT device being different or the surrounding environment being inappropriate. Using this problem as example, we detail below how our proposal responds. In this configuration, Bluetooth low energy (BLE) beacons are utilized as the source of metadata in order to manage the locations of sensor devices [22], [23]. The IoT device periodically sends a camera image as sensor data to the gateway via IEEE 802.11. Moreover, the IoT device writes the beacon information (i.e. location metadata) received via the BLE device into the vendor-specific extension of the PRQ frame and sends it separately from the sensor data. Here, the beacon information means the universally unique identifier (UUID), Major value, Minor value, and received signal strength indicator (RSSI) unique to the BLE beacon; this requires 21 bytes per beacon [24]. Since multiple beacons must be acquired to determine position, they are written in the same vendor-specific extension and aggregated in one PRQ frame. At the gateway, an IoT device identifier and a gateway identifier are assigned to the beacon information, and the beacon information is transmitted to the management server.

The systematic collection of metadata in addition to sensing data as described above, ensures the metadata can be used for management of the sensor itself and the sensor data.

B. ADVANTAGES OF THE PROPOSAL

Low-layer metadata collection using PRQ does not depend on the high-level protocol stack, so it offers the following advantages.

- Low power consumption
- Low computing load
- Time sensitivity
- Independent of IP communication establishment

Normally, the management protocol for maintaining the connection operates in the protocol stack above the network layer [25]. Flexible network management and control is realized by using high-level protocols. However, this consumes power and computing resources to maintain communication [26].

In particular, inexpensive devices in the market and mobility-type battery driven devices require operation with limited power consumption and computing resources. Our PRQ-based approach reduces power consumption and computing load by eliminating the need for management protocols and layer processing associated with these network connections. Also, network processing in the high-level

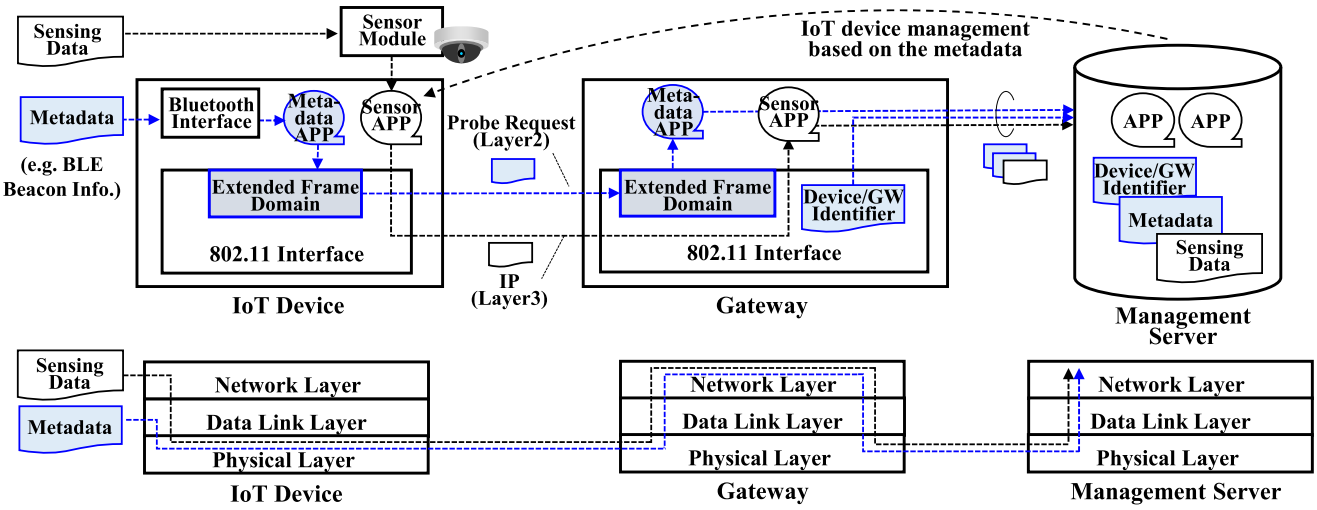

FIGURE 2. Proposed low-layer metadata collection scheme.

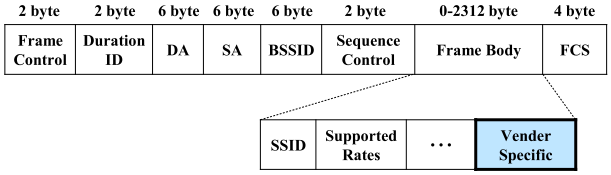

FIGURE 3. Probe request frame body of IEEE 802.11.

protocol stack described above increases delays in metadata transfer. However, our proposal eliminates the need for these network processes contributing to reducing the time required for metadata transfer.

In addition to the above, another important advantage is its independence from the communication connection. For example, if data is uploaded intermittently, the sleep state is often triggered to reduce power consumption. Normally, when resuming data communication from a deep sleep state in which the network connection is not maintained, connection initiation processes such as authentication, association, encryption, and Internet Protocol (IP) address reassignment are required [27]. However, since our proposal dispenses with these processes, it enables immediate metadata collection independent of network connection. This also offers an advantage for IoT device management. Information related to the device can be collected as metadata in advance before the communication connection though the protocol of the Network layer or higher. This means that it is possible to assign the communication connection settings of the protocol stack above the IP layer according to the metadata. As an example, the location metadata of the device is used to implement network settings to suit the deployment area of the device. Network segments and IP address grouping can be flexibly assigned to each device deployment area. These settings are also assigned for the initial connection to the network and connection recovery from deep sleep.

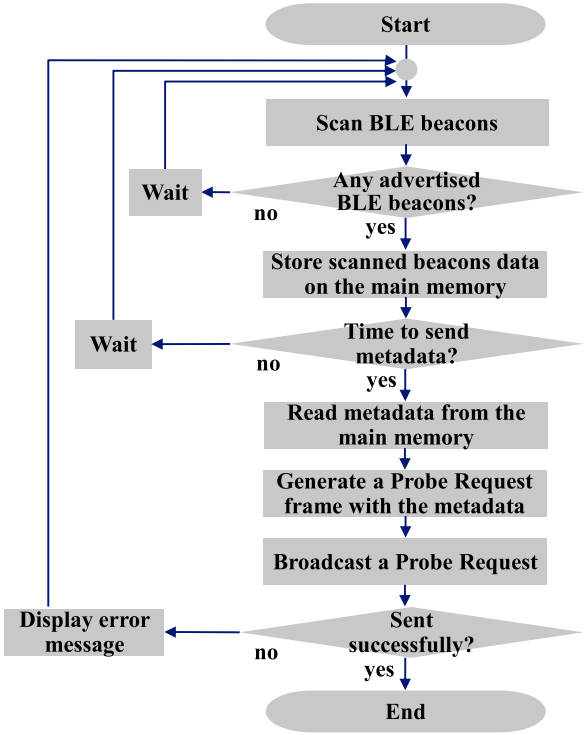

FIGURE 4. Processing metadata transmission programs implemented in IoT devices.

IV. IMPLEMENTATION

We detail here an implementation of collecting location metadata (i.e., BLE beacons) using the proposed system shown in Fig. 2. Fig. 4 shows the process based on the metadata sender program set in the IoT device. It shows the sequence of processes from scanning the BLE beacon signal to sending the PRQ frame. The IoT device scans for BLE beacons and stores the detected beacon data (UUID, major, minor, RSSI) in its main memory when a beacon is detected. Here, BLE beacons are emitted using a 100 ms cycle, and the IoT device

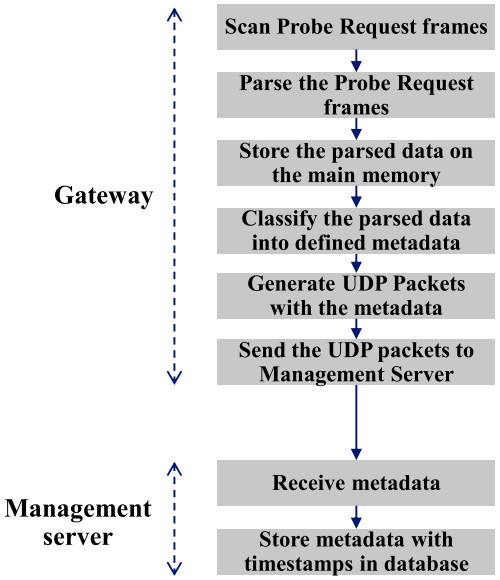

FIGURE 5. Processing of metadata receiving programs implemented in Gateway and Management Server.

scans for beacon signals on a 2 s cycle. The total amount of beacon information per beacon occupies 21 bytes. The temporarily stored metadata is read from the main memory in accordance with the periodic metadata sending time. The metadata is then stored in the frame body of the PRQ frame and broadcast. The transmission cycle of the PRQ frame is set to 2 s. These series of metadata transmission processes are executed repeatedly.

Figure 5 shows the processing of the Metadata receiver program implemented on the Gateway and Management Server side. It shows the process from the scanning of PRQ frames to the reception of metadata at the Management Server. First, the Gateway scans PRQ frames; when the Gateway receives PRQ frames, it parses them. The parsed metadata is stored in the main memory of the gateway along with the Mac address for IoT device identification. If the predefined metadata exists, the gateway generates a UDP packet. The metadata is stored in the data frame of the UDP packet and sent to the management server. When the management server receives the metadata, it stores the metadata in a database with a timestamp.

To realize the above processes, MM-BLEBC1 was used as the BLE beacon, and an ESP32 (ESP-WROOM-32) with IEEE 802.11n and bluetooth v4.2 communication modules was used as the IoT device [28]. A Raspberry-pi was used as the gateway [29].

V. EVALUATION

A. CPU UTILIZATION AND POWER CONSUMPTION FOR METADATA COLLECTION

An evaluation was performed to show the effectiveness of the proposal in terms of computing load and power consumption. Fig. 6 shows the measurement configuration. We investigated the load and power consumption when collecting metadata of IoT devices and passing the data to the gateway. Seven BLE beacons, which is the maximum number that can be carried by one PRQ frame, were used as metadata sources; their BLE beacon information was used as the metadata. As shown in Fig. 6, metadata was sent to the Gateway in both PRQ-based and IP-based cases for comparison. CPU utilization and power consumption in each case were measured by the Monitoring PC. Here, the transmission cycle of metadata in the PRQ-based scheme used the values described in the previous section. The transmission cycle for IP-based packets was set to 2 s. This is the same value used in the PRQ-based scheme. Open source libraries were used for the IP-based implementation [30], [31], [32].

We compared the CPU utilization of the cores for metadata transmission in the IP-based and PRQ-based schemes. Fig. 7 shows a bar graph of the average CPU utilization over a 10-minute period. The IP-based scheme showed an average utilization of 41.1%, while the PRQ-based scheme showed a lower utilization, 29.4%. In terms of reduction, this means a reduction of 28.5%.

Furthermore, the power consumption of both schemes associated with metadata transmission was compared. Fig. 8 plots power consumption over time. The IP-based scheme often created bursts in power consumption. This is due to the management protocols needed to maintain connectivity, such as Wi-Fi keep-alive, Address Resolution Protocol (ARP), and Internet Control Message Protocol (ICMP). The frequency of these management protocol events increases as the number of devices in the WLAN increases. Therefore, power bursts are likely to occur frequently. On the other hand, the PRQ-based scheme yielded no burst-like increases in power consumption. Fig. 9 shows the cumulative distribution functions (CDF) for the power consumption of the two schemes. The results in Fig. 8 were statistically analyzed. From the CDF data, it can be seen that the IP-based scheme often consumed over 900 mW unlike the PRQ-based scheme. With regard to average value, IP-based scheme consumed 801.12 mW while the PRQ-based scheme consumed 761.64 mW. This lack of peaks in the power consumption suggest that the proposal will be very effective in sensor devices with limited maximum power supplies.

B. TIME SENSITIVITY

An evaluation was performed to demonstrate the validity of the proposal in terms of time sensitivity. Notably, sleep states are often set for each IoT device to help reduce power consumption. In particular, in the sleep mode where the power consumption is greatly reduced, the wireless chip is hibernated and the network connection is dropped. Therefore, the delays required to wake up from sleep mode and send metadata were compared for the IP-based and PRQ-based schemes. The processing time in a series of flows that collected IoT device metadata and upload it to the gateway was measured. Fig. 10 shows the configuration used in the evaluation. Similar to the power consumption measurement

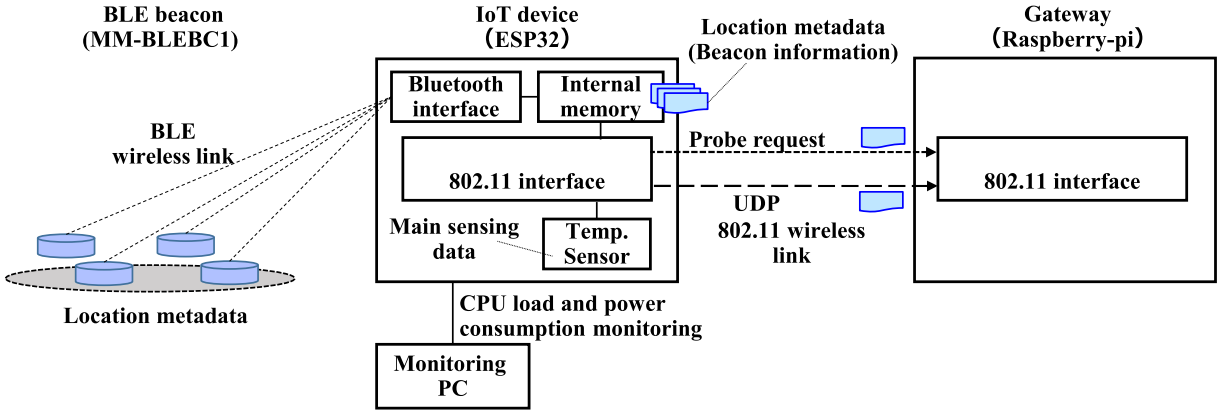

FIGURE 6. Measurement configuration of CPU utilization and power consumption.

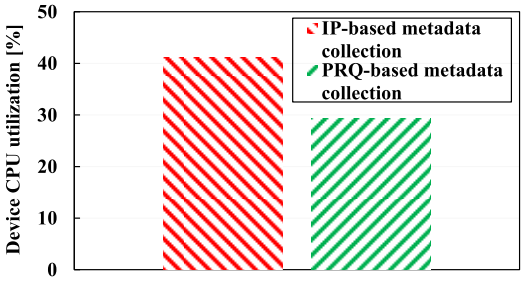

FIGURE 7. Comparison of IP-based and PRQ-based average device CPU utilization monitoring result.

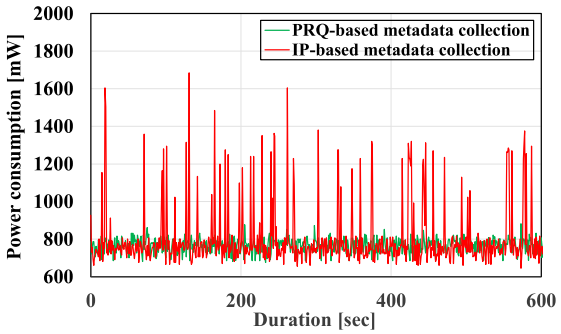

FIGURE 8. Power consumption monitoring results versus time.

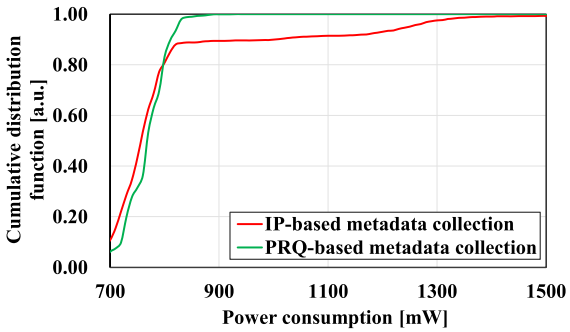

FIGURE 9. Cumulative distribution function (CDF) of power consumption.

in Fig. 6, a total of seven BLE beacons are used for location metadata. ESP32 was used for the IoT device. In addition, a Raspberry-pi was used as the gateway with a dynamic host configuration protocol (DHCP) server function. In addition to an IEEE 802.11 wireless link, a general purpose input/output (GPIO) wired link was set between IoT device and gateway. This is used to send a trigger signal to notify the start of measurement.

Fig. 11 shows the detailed flow for metadata transfer. Normally, in IP-based metadata collection, PRQ, authentication, association, encryption, and IP address assignment are executed in order. After that, the metadata is extracted from the internal memory, stored in the UDP frame, and then sent to the Gateway. On the other hand, in the PRQ-based scheme, metadata is transmitted without performing the processes such as authentication, association, encryption, and IP address allocation. After receiving the trigger signal, the internal memory is accessed, the metadata is extracted, stored in the PRQ frame, and transmitted to the Gateway. Therefore, the proposal is expected to achieve shorter transfer times than the IP-based scheme.

As shown in Fig.11, the time taken to collect metadata by the IP-based scheme, Δt_{ip}, is given by the following equation.

$$\Delta t_{ip} = t_{ip} - t_{trig} \tag{1}$$

where t_{ip} represents the metadata arrival time in the IP-based scheme, and t_{trig} represents the time of receipt of the trigger signal. The time required for metadata transmission by the proposal is Δt_{probe}, and is given by the following equation.

$$\Delta t_{probe} = t_{probe} - t_{trig} \tag{2}$$

where t_{probe} represents the metadata arrival time. Equations (1) and (2) were used to evaluate the metadata collection delay.

Figure 12 shows a comparison of the delays imposed in collecting metadata. The bar chart shows mean values and 95% confidence intervals. The IP-based scheme takes an average of 913.43 ms with a wider 95% confidence interval than the PRQ-based scheme. On the other hand, the mean for the PRQ-based scheme was 92.78 ms. The deep sleep state, which drops the wireless connection link, significantly reduces power consumption but delays data collection. The

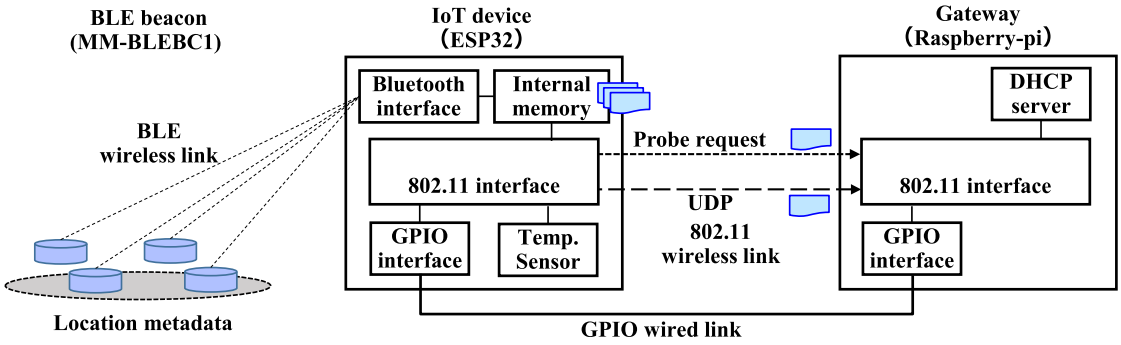

FIGURE 10. Measurement configuration for metadata collection delay.

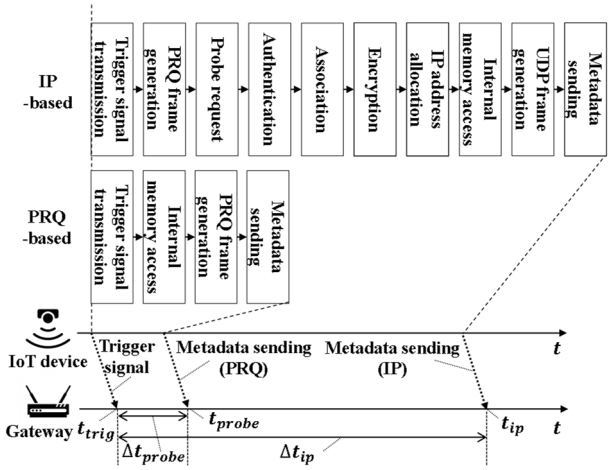

FIGURE 11. Graphical understanding of IP-based and PRQ-based metadata collection flow and delay.

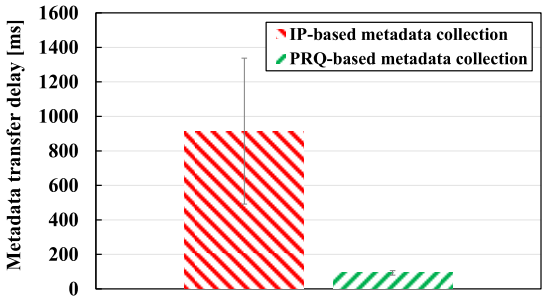

FIGURE 12. Comparison of IP-based and PRQ-based metadata collection delay.

need to discard memory information in the device in the case of deep sleep requires initializing the Wi-Fi chip for sleep recovery. Therefore, there is a certain processing delay with both schemes. However, it was found that the proposal achieves a reduction in delay of 89.8% compared to the IP-based scheme.

C. IP CONNECTION-INDEPENDENT METADATA COLLECTION

One of the advantages of layer-2 based low layer collection is the ability to perform IP connection-independent metadata collection. This means that the location, state and peripheral state of the device can be collected in advance without depending on the network connection. This allows the device's network settings to flexibly reflect the device's status. Therefore, we implemented a management system that uses PRQ-based metadata collection to manage IoT networks and devices, and confirmed its feasibility. As an example of managing IoT networks and devices, when location-specific metadata is collected, predetermined IP address segments and ranges are assigned to each area according to the location metadata. Since the data used does not depend on IP connections, assignment will proceed even before completion of initial NW connection or when the device is relocated. System behavior was evaluated for initial device connectivity and subsequent device relocation.

Figure 13 shows the configuration of the IoT network management system. IoT devices were deployed in area #1 and area #2. Here, it is assumed that area # 1 and area # 2 are under the same gateway but are physically separated. All IoT devices acquire temperature, which is the sensor data, and periodically send the sensing data to the management server. Area #1 and area #2 are equipped with BLE beacons whose positions are managed in advance as metadata sources The IoT device stores the beacon information (UUID, major, minor, RSSI) of the BLE beacon signal as location metadata in the PRQ and periodically sends it to the gateway.

Sensing data and location metadata are collected by the management server. The management server extracts the beacon with the maximum RSSI and collates it with the beacon position to roughly grasp the position of the IoT device. Depending on the location-based metadata sent by the IoT device, the management server dynamically assigns the IP address of the network according to the location of the device, and further visualizes the logical topology.

We evaluated scenarios with three states. In state 1, which is the initial state, device #1 and device #3 are deployed in area #1 and area #2, respectively. However, device #2 is deployed outside the gateway coverage. By relocating device #2 to area #1, state 1 transitions to state 2. After transitioning to state 2, device #2 receives the BLE beacon of area #1 and transfers it to the Gateway via PRQ as location metadata. The management server collects the metadata, immediately

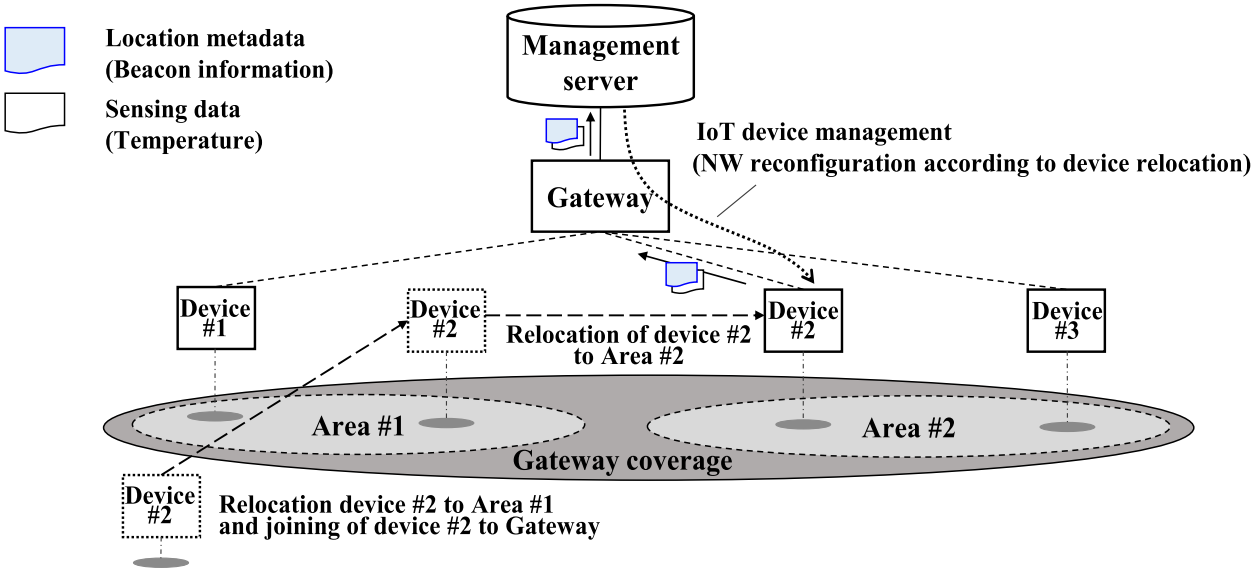

FIGURE 13. Configuration diagram of the implemented network management system utilizing PRQ-based metadata collection.

assigns the appropriate IP address to device #2 according to the metadata, and connects it to the network. Here, the IP address assigned to device #2 in area #1 is taken from the range of 192.168.222.11 to 192.168.222.19 according to a predetermined rule. Furthermore, by relocating device #2 from area #1 to area #2, state 2 transitions to state 3. After transitioning to state 3, device #2 receives the BLE beacon of area #2 and transfers it to the Gateway via PRQ as location metadata. The management server collects the metadata and immediately reassigns the IP address of device #2 according to the metadata. Here, the IP address assigned to device #2 in area #2 taken from the range of 192.168.222.21 to 192.168.222.29 according to a predetermined rule.

Figure 14 shows screenshots of the logical network topology diagram displayed on the actual management screen. The IP address, mac address, collected main sensing data, and metadata of the devices in the network are managed by a database, and the logical network topology diagram is generated as a JavaScript Object Notation (JSON) file based on these results. (a), (b) and (c) show the three states, 1 to 3. (a) indicates state 1, and device #2 exists outside the Gateway coverage. State 2 is entered when device #2 relocates to area #1 and joins the network. State 3 indicates that device #2 has been relocated to area #2 and the IP address has been reassigned. The screenshot of the management screen visually confirms that management of the logical network topology according to the location was correctly performed for the relocation of device #2.

Figure 15 shows a time series log for device #2 on the management server. The state transition from state 1 to state 3 was actually performed and the time series log was captured.

The time series log outputs information such as received metadata, device Mac address, and IP address. Fig. 15 confirms that the metadata sent from device #2 was received after the transition from state 1 to state 2. The received metadata,

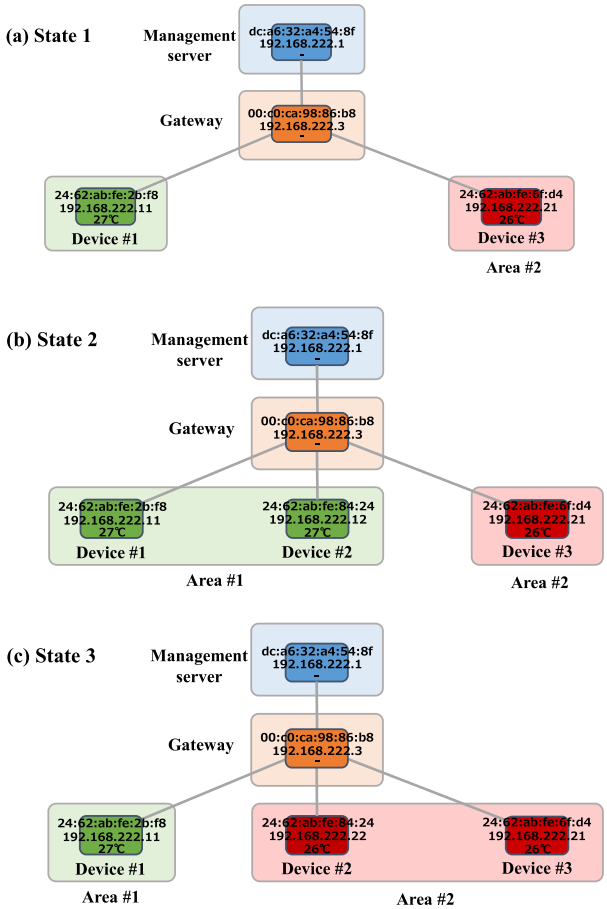

FIGURE 14. Physical and logical network management screen diagram created by the management server.

totaling 21 Bytes, consists of UUID/ Major value/ Minor value/ RSSI for the BLE beacon. Based on this metadata, IP address [192.168.222.12] was assigned to device #2. After

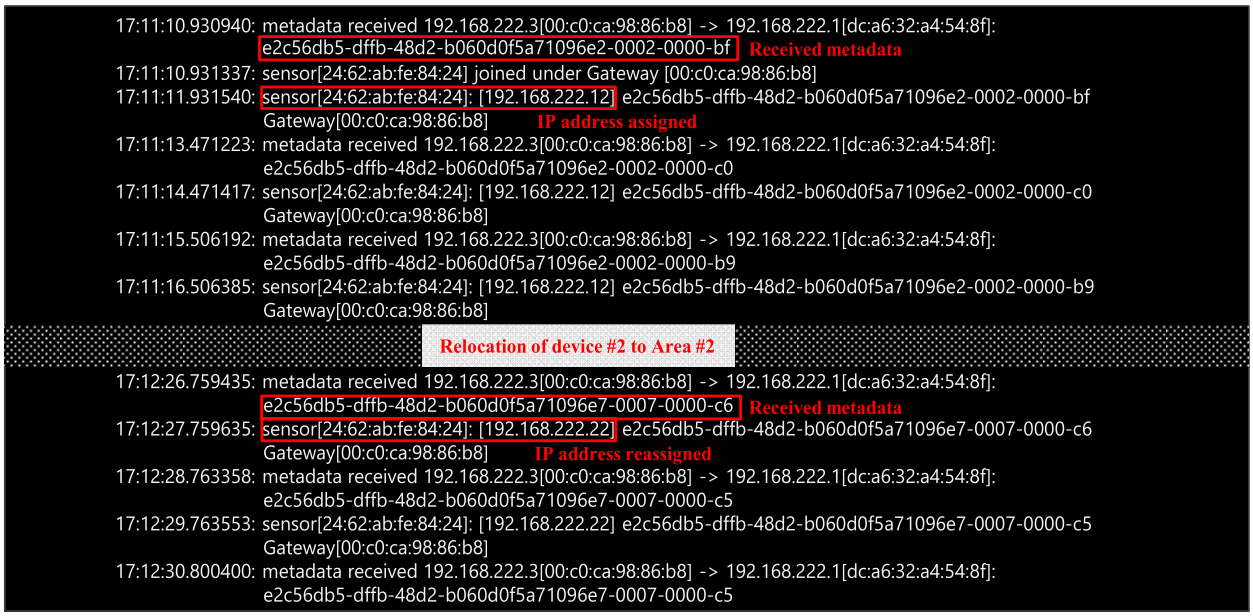

FIGURE 15. Time series log of device #2 output on the management server.

transitioning to state 3, it was confirmed that metadata with a UUID different from that of state 2 was received. Based on this metadata, it was confirmed that a new IP address [192.168.222.22] was assigned.

These results are for a small number of BLE beacons. Naturally, it is expected that the introduction of a location identification algorithm, which is currently being actively researched, will dramatically improve the location identification of devices in this system [33], [34], [35], [36]. However, the details of the positioning algorithm are different from the main scope of this paper. Therefore, this evaluation focused on confirming the feasibility of metadata collection and utilization. With regard to future prospects, it is necessary to show that usability can be improved in combination with existing localization algorithms to accommodate a variety of use cases.

VI. FUTURE SCOPE AND CHALLENGES

There are several aspects to the future challenges facing the proposed system. One is security. The proposed system uses the layer-2 protocol Probe Request to transfer device-specific metadata to the GW. Since metadata can be collected even before an IP connection is established, the metadata can be used for network management, including the IP address of the device. However, since metadata contains device-specific information, security concerns must be addressed to avoid the risk of device identification. Various solutions have been proposed in recent years against the security risks targeting Probe Requests. For example, mac address randomization is one solution [44]. In order to utilize this security protocol in the proposed system, additional implementation is required in terms of linking target devices, main sensing data and metadata. In addition, one direction is to consider new lightweight security protocols, rather than relying on existing security protocols.

Another aspect is feasibility evaluation in actual IoT service fields. Actual service fields are diverse for each service, and there are environmental variables such as the number of IoT devices and radio frequency interference. Therefore, in order to improve the system's practicality, it is necessary to deploy the system in actual service delivery environments and conduct dynamic system evaluations. For example, parameters that strongly depend on environmental factors, such as frame collisions and delays in high device-density situations with a large number of IoT devices, and the optimal frequency of metadata frame collection for each application, need to be studied in detail.

VII. CONCLUSION

We have proposed a novel IoT metadata collection scheme for wireless local area network (WLAN) environments to enhance device management and control by utilizing metadata that represents device-specific information. Our proposal utilizes the extended region of WLAN probe request (PRQ) frames, a layer-2 protocol, to collect metadata. This enables metadata collection in low-layer communication without modifying existing protocols. We show that low-layer metadata collection reduces the device central processing unit (CPU) load and suppresses burst power consumption caused by high-layer management protocols, and so is superior to conventional Internet Protocol (IP) -based metadata collection (layer-3 protocols and above). In addition, in terms of time sensitivity, the collection delay on deep sleep exit was reduced by 89.8%. Furthermore, we implemented a network management system that leveraged PRQ-based metadata collection as an example of metadata-based management of Internet of Things (IoT) networks and devices,

and confirmed its feasibility. Experiments showed that our proposal permitted network topology configurations to be realized by collecting metadata in the background, without relying on network connectivity over layer-3 protocols, while taking into account the location and state of devices. Finally, we indicated that future work on this proposal includes both security aspects and a detailed evaluation in real service environments. To strengthen the security aspect of the proposal, it is necessary to apply a security protocol that can handle Probe Request. In addition, a feasibility study in a real service site with a variety of environmental factors such as the number of devices and radio interference is required.

REFERENCES

[1] M. Burhan, R. Rehman, B. Khan, and B.-S. Kim, "IoT elements, layered architectures and security issues: A comprehensive survey," *Sensors*, vol. 18, no. 9, p. 2796, Aug. 2018.

[2] D. Ma, G. Lan, M. Hassan, W. Hu, and S. K. Das, "Sensing, computing, and communications for energy harvesting IoTs: A survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1222–1250, 2nd Quart., 2020.

[3] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on Internet of Things from industrial market perspective," *IEEE Access*, vol. 2, pp. 1660–1679, 2014.

[4] S. Al-Sarawi, M. Anbar, R. Abdullah, and A. B. Al Hawari, "Internet of Things market analysis forecasts, 2020–2030," in *Proc. 4th World Conf. Smart Trends Syst., Secur. Sustainability (WorldS)*, Jul. 2020, pp. 449–453.

[5] N. Nesa, T. Ghosh, and I. Banerjee, "Outlier detection in sensed data using statistical learning models for IoT," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Apr. 2018, pp. 1–6.

[6] M. A. Bhatti, R. Riaz, S. S. Rizvi, S. Shokat, F. Riaz, and S. J. Kwon, "Outlier detection in indoor localization and Internet of Things (IoT) using machine learning," *J. Commun. Netw.*, vol. 22, no. 3, pp. 236–243, Jun. 2020.

[7] M. Zhang, X. Li, and L. Wang, "An adaptive outlier detection and processing approach towards time series sensor data," *IEEE Access*, vol. 7, pp. 175192–175212, 2019.

[8] M. Milenkovic, "IoT data models and metadata," in *Internet of Things: Concepts and System Design*. Cham, Switzerland: Springer, 2020, pp. 201–223, doi: 10.1007/978-3-030-41346-0_6.

[9] R. Zheng, H. Wang, and J. Zhao, "A unified management framework for EIoT systems based on metadata and event detection," *IEEE Access*, vol. 7, pp. 112629–112638, 2019.

[10] A. Kiourtis, A. Mavrogiorgou, and D. Kyriazis, "Prioritization of IoT devices healthcare data based on attribute scoring and metadata annotation," in *Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT)*, Aug. 2021, pp. 213–220.

[11] D. Ballari, M. Wachowicz, and M. A. M. Callejo, "Metadata behind the interoperability of wireless sensor networks," *Sensors*, vol. 9, no. 5, pp. 3635–3651, May 2009.

[12] Y. Park, J. Choi, and J. Choi, "Conceptual metadata model for sensor data abstraction in IoT environments," *IOP Conf. Ser., Mater. Sci. Eng.*, vol. 383, no. 1, 2018, Art. no. 012013.

[13] H. Jeung, S. Sarni, I. Paparrizos, S. Sathe, K. Aberer, N. Dawes, T. G. Papaioannou, and M. Lehning, "Effective metadata management in federated sensor networks," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous, Trustworthy Comput.*, Jun. 2010, pp. 107–114.

[14] N. Honle, U.-P. Kappeler, D. Nicklas, T. Schwarz, and M. Grossmann, "Benefits of integrating meta data into a context model," in *Proc. 3rd IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Mar. 2005, pp. 25–29.

[15] M. Abu-Elkheir, M. Hayajneh, and N. A. Ali, "Data management for the Internet of Things: Design primitives and solution," *Sensors*, vol. 13, no. 11, pp. 15582–15612, Nov. 2013.

[16] K. Wrona and M. Jarosz, "Use of blockchains for secure binding of metadata in military applications of IoT," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Apr. 2019, pp. 213–218.

[17] Z. Luo, Z. Li, S. Luan, W. Zhuang, and J. Yang, "Metadata-based automated IoT device management system: Demo abstract," in *Proc. 1st Int. Workshop Cyber-Phys.-Hum. Syst. Design Implement.*, May 2021, pp. 19–20.

[18] U. Hassan, M. Bassora, A. H. Vahid, S. O'Riain, and E. Curry, "A collaborative approach for metadata management for Internet of Things: Linking micro tasks with physical objects," in *Proc. 9th IEEE Int. Conf. Collaborative Comput., Netw., Appl. Worksharing*, Oct. 2013, pp. 593–598.

[19] *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks-Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, Standard 802.11-2016, Dec. 2016.

[20] L. Davoli, L. Belli, A. Cilfone, and G. Ferrari, "From micro to macro IoT: Challenges and solutions in the integration of IEEE 802.15.4/802.11 and sub-GHz technologies," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 784–793, Apr. 2018.

[21] J. Sheth, C. Miremadi, A. Dezfouli, and B. Dezfouli, "EAPS: Edge-assisted predictive sleep scheduling for 802.11 IoT stations," *IEEE Syst. J.*, vol. 16, no. 1, pp. 591–602, Mar. 2022.

[22] K. E. Jeon, J. She, P. Soonsawad, and P. C. Ng, "BLE beacons for Internet of Things applications: Survey, challenges, and opportunities," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 811–828, Apr. 2018.

[23] M. Haus, A. Y. Ding, and J. Ott, "Managing IoT at the edge: The case for BLE beacons," in *Proc. 3rd Workshop Exper. With Design Implement. Smart Objects*, Oct. 2017, pp. 41–46.

[24] P. Spachos and K. Plataniotis, "BLE beacons in the smart city: Applications, challenges, and research opportunities," *IEEE Internet Things Mag.*, vol. 3, no. 1, pp. 14–18, Mar. 2020.

[25] P. G. Zaware and S. V. Shinde, "Wireless monitoring, controlling and firmware upgradation of embedded devices using Wi-Fi," in *Proc. Int. Conf. Adv. Commun. Comput. Technol. (ICACACT)*, Aug. 2014, pp. 1–6.

[26] A. Rice and S. Hay, "Decomposing power measurements for mobile devices," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. (PerCom)*, Apr. 2010, pp. 70–78.

[27] J. Mesquita, D. Guimarães, C. Pereira, F. Santos, and L. Almeida, "Assessing the ESP8266 WiFi module for the Internet of Things," in *Proc. IEEE 23rd Int. Conf. Emerg. Technol. Factory Autom. (ETFA)*, vol. 1, Sep. 2018, pp. 784–791.

[28] A. Maier, A. Sharp, and Y. Vagapov, "Comparative analysis and practical implementation of the ESP32 microcontroller module for the Internet of Things," in *Proc. Internet Technol. Appl. (ITA)*, Sep. 2017, pp. 143–148.

[29] (Apr. 2022). *Raspberry Pi 3 Model B*. [Online]. Available: https://www.raspberrypi.org/products/raspberry-pi-3-model-b/

[30] (Nov. 2020). *Espressif Systems CO., LTD, ESP-IDF Programming Guide Release v4.1*. [Online]. Available: https://docs.espressif.com/projects/esp-idf/en/v4.1/index.html

[31] (Dec. 2021). *Source Code for ESP32 Wi-Fi Support*. [Online]. Available: https://github.com/espressif/arduino-esp32/blob/master/libraries/WiFi/src/WiFi.h

[32] (Dec. 2019). *Arduino WiFi Shield Library* [Online]. Available: https://www.arduino.cc/en/Reference/WiFi

[33] C. Xiao, D. Yang, Z. Chen, and G. Tan, "3-D BLE indoor localization based on denoising autoencoder," *IEEE Access*, vol. 5, pp. 12751–12760, 2017.

[34] S. Sadowski and P. Spachos, "RSSI-based indoor localization with the Internet of Things," *IEEE Access*, vol. 6, pp. 30149–30161, 2018.

[35] S. Sadowski and P. Spachos, "Optimization of BLE beacon density for RSSI-based indoor localization," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, May 2019, pp. 1–6.

[36] A. D. Blas and D. López-de-Ipiña, "Improving trilateration for indoors localization using BLE beacons," in *Proc. 2nd Int. Multidisciplinary Conf. Comput. Energy Sci. (SpliTech)*, Jul. 2017, pp. 1–6.

[37] M. Bukhsh, S. Abdullah, and I. S. Bajwa, "A decentralized edge computing latency-aware task management method with high availability for IoT applications," *IEEE Access*, vol. 9, pp. 138994–139008, 2021.

[38] A. Ahmed, S. Abdullah, M. Bukhsh, I. Ahmad, and Z. Mushtaq, "An energy-efficient data aggregation mechanism for IoT secured by blockchain," *IEEE Access*, vol. 10, pp. 11404–11419, 2022.

[39] F. Tavakolizadeh and S. Devasya, "Thing directory: Simple and lightweight registry of IoT device metadata," *J. Open Source Softw.*, vol. 6, no. 60, p. 3075, Apr. 2021.

[40] P. R. S. Bhama and C. P. Jayabal, "MetaInfoChain : Bi-layered blockchain consensus for metadata aggregation in IoT and cloud environments," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 12, Sep. 2021, Art. no. e4362.

[41] F. Tasmin Jaigirdar, C. Rudolph, and C. Bain, "Prov-IoT: A security-aware IoT provenance model," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Jan. 2021, pp. 1360–1367.
[42] X. Huang, J. Fan, Z. Deng, J. Yan, J. Li, and L. Wang, "Efficient IoT data management for geological disasters based on big data-turbocharged data lake architecture," *ISPRS Int. J. Geo-Inf.*, vol. 10, no. 11, p. 743, Nov. 2021.
[43] L. de la Torre, J. Chacon, D. Chaos, R. Heradio, and R. Chandramouli, "Using IoT-type metadata and smart web design to create user interfaces automatically," *IEEE Trans. Ind. Informat.*, early access, Jun. 27, 2022, doi: 10.1109/TII.2022.3186638.
[44] J. Tan and S.-H. Gary Chan, "Efficient association of Wi-Fi probe requests under MAC address randomization," in *Proc. IEEE INFOCOM Conf. Comput. Commun.*, May 2021, pp. 1–10.

RYOTA SHIINA (Member, IEEE) received the M.E. degree in material science and engineering from the Tokyo Institute of Technology, Tokyo, Japan, in 2014, and the Ph.D. degree from the Graduate School of Information Science and Technology, Osaka University, Japan, in 2022. In 2014, he joined the NTT Access Network Service Systems Laboratories, where he has been engaged in research on optical access network systems and wireless access network systems. He is a member of IEICE. He received the Young Researcher's Award from the Institute of Electronics, Information, and Communication Engineers (IEICE), Japan, in 2018, and the Encouraging Award from IEICE Technical Committee on Communication Systems (CS), in 2017.

SHINYA TAMAKI received the M.E. degree in precision engineering from the University of Tokyo, Tokyo, Japan, in 2009. He joined the NTT Access Network Service Systems Laboratories, in 2009, where he was involved in the research and development of next-generation optical access systems. His current research interests include the system architecture of edge computing and the Internet of Things, including automated IoT devices provisioning, data trustworthiness, and cyber physical services.

CHE HUANG received the bachelor's and Master of Arts and Sciences degrees from Osaka Kyoiku University, in 2013 and 2015, respectively, and the Ph.D. degree from the Nara Institute of Science and Technology (NAIST), in 2018. He joined the NTT Access Network Service Systems Laboratories, in 2018, where he was involved in the research and development of optical access systems mainly related to automatic network management and network virtualization. He is a member of IEICE.

TOMOYA HATANO received the B.E., M.E., and Ph.D. degrees from Keio University, Tokyo, Japan, in 2002, 2004, and 2007, respectively. In 2004, he joined the NTT Access Service Systems Laboratories. He is engaged in the research and development of optical communication systems and network virtualization.

TAKASHI YAMADA received the B.E., M.E., and Ph.D. degrees in electrical engineering from Hokkaido University, Sapporo, Japan, in 1997, 1999, and 2003, respectively. In 2003, he joined the NTT Access Network Systems Laboratories, Chiba, Japan, where he was involved in the research of energy efficient optical access network systems. From 2013 to 2016, he was at the Research and Development Planning Department, NTT Information Network Laboratory Group, where he was involved in Public Relations and Information Strategy. His current research interest includes virtualization of optical access networks.

TATSUYA SHIMADA received the B.E. degree in applied physics from Tohoku University, Sendai, Japan, in 1997, and the Ph.D. degree from Hokkaido University, Sapporo, Japan, in 2009. In 1997, he joined the NTT Multimedia Systems Development Center, Chiba, Japan, where he was engaged in the development of ATM optical access systems. In 1999, he moved to the NTT Access Network Service Systems Laboratories, Chiba. Since 2000, he has been working on WDM optical access network and systems. Since 2014, he has been working on an optical network for 5G and future mobile system. He is a member of the Institute of Electronics, Information and Communication Engineers, Japan.

TOMOHIRO TANIGUCHI received the B.E. and M.E. degrees in precision engineering from the University of Tokyo, Tokyo, Japan, in 2000 and 2002, respectively, and the Ph.D. degree in electrical, electronic and information engineering from Osaka University, Osaka, Japan, in 2010. In 2002, he joined the NTT Access Network Service Systems Laboratories, where he has been engaged in research on optical access systems mainly related to optical heterodyne technologies, radio-on-fiber transmission, and video distribution systems.