IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 14 October 2023, accepted 12 November 2023, date of publication 28 November 2023,
date of current version 1 December 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3335273

RESEARCH ARTICLE

Implementation and Evaluation of the Control Mechanism Among Distributed MQTT Brokers

KAZUHIRO KOSAKA[1], YUTO NODA[2], TETSUYA YOKOTANI[3], (Member, IEEE), AND KOICHI ISHIBASHI[4], (Member, IEEE)

[1] Graduate School of Electrical Engineering and Electronics, Kanazawa Institute of Technology, Nonoichi, Ishikawa 921-8501, Japan
[2] Mitsubishi Electric Information Network Corporation, Tokyo 108-0023, Japan
[3] Department of Electrical and Electronic Engineering, College of Engineering, Kanazawa Institute of Technology, Nonoichi, Ishikawa 921-8501, Japan
[4] Department of Information and Computer Science, College of Engineering, Kanazawa Institute of Technology, Hakusan-shi, Ishikawa 924-0838, Japan

Corresponding authors: Kazuhiro Kosaka (c6201098@st.kanazawa-it.ac.jp) and Tetsuya Yokotani (yokotani@neptune.kanazawa-it.ac.jp)

ABSTRACT MQTT for IoT communication requires multiple brokers to aggregate traffic from localized areas. However, routing mechanisms among these brokers have yet to be specified. In this paper, the Distributed MQTT broker by data Link look-up for Traffic reduction (DMLT) is proposed as a new routing mechanism. This mechanism is aimed at layer-2 based control. It provides cooperation with MQTT and the Spanning Tree Protocol and invokes a traffic reduction and simplified transfer by an independent flow. We evaluate the performance of the DMLT method and compare the DMLT method and the conventional method in terms of traffic volume. According to the experimental results, a reduction in traffic volume is confirmed. We also build and verify a prototype of a wide-area DMLT (WDMLT) system, which is a method suitable for large-scale deployment of DMLT. Finally, the IoT DEP registered as an international standardization and its application to the proposed method is explained.

INDEX TERMS IoT, MQTT, multiple brokers, routing protocol, VPN.

I. INTRODUCTION

IoT services have been diversifying in recent years because IoT has become widespread in various fields for example industrial and consumer fields. Accordingly, the number of IoT devices is predicted to increase from 32.4 billion in 2022 to 44 billion in 2025 [1]. Traffic is expected to increase due to the growing number of IoT devices. However, when the traditional Internet is applied to IoT communications, data transfer through a large number of networked devices becomes difficult because the Internet provides IP-type routing and requires a domain name system to translate data locations and IP addresses [2]. Therefore, IP-independent networks are expected [3].

One candidate solution is Message Queueing Telemetry Transport (MQTT) [4], MQTT is a Pub/Sub type communication by way of a ''Broker''. Therefore, multiple brokers are needed to accommodate traffic from various areas [5]. However, the discussion of this distributed MQTT Broker is undecided. Therefore, the author proposes a routing method that utilizes the data link layer to reduce the increasing traffic. This method is called the Distributed MQTT brokers by data Link lookup for Traffic reduction (DMLT) [6].

In this paper, a prototype of the DMLT is implemented and compared with a conventional method in terms of traffic volume. Next, Wide-area Distributed MQTT brokers by data Link lookup for Traffic reduction (WDMLT) is introduced for operation in wide-area networks. Finally, the adaptation to IoT DEP, which is currently standardized by ISO/IEC JTC1/SC41 as ISO/IEC30161 series, is discussed.

II. RELATED WORKS

MQTT consists of a Publisher (e.g., a sensor device), a Subscriber, and a Broker that mediates between the Publisher and the Subscriber. The specific communication method is described using Figure 1.

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

First, the Publisher assigns a Topic to the data and sends it to the Broker (Figure 1 (1)). This Topic can be specified by any name, and the Broker can identify the data based on this Topic. The Broker temporarily stores the Topic. The Broker sends a Topic to the Subscriber when the Topic it stores matches the requested Topic (Figure 1 (3)). Different subscribers can also request the same Topic and receive it from the Broker. MQTT has lower packet size and overhead than the conventional Internet protocols [7]. Taking advantage of these characteristics, MQTT is being researched and analyzed for implementation in IoT devices that require large amounts of data [8]. However, in the case of large-scale deployments that require deployment over a wide area, it is necessary to prepare multiple Brokers [9] with a routing control function. Several approaches have been proposed for this routing function, including the multicast method among clustered Brokers [10] and the conventional IP-based routing method [11]. However, the developed method has not yet been specified: in the study of using multiple Brokers in MQTT, the Interworking Layer of Distributed MQTT Brokers (ILDM) [5] is a technique to relay messages between arbitrary Brokers. This technology can relay messages from Publishers using Brokers with ILDM functionality.

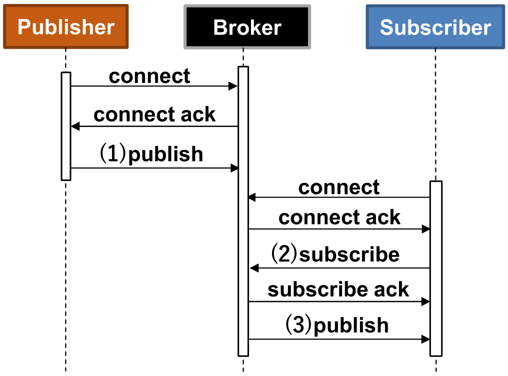


FIGURE 1. Overview of MQTT communication sequence.

Figure 2 shows the communication sequence including ILDM. This ILDM is a Broker that has the functions of both a publisher and a subscriber and can connect to other Brokers (1). Broker with ILDM functionality forwards this message to other Brokers (2). All Brokers with ILDM capabilities can then share the data created by the Publisher. Subscriber, on the other hand, is the same as MQTT in Figure 1. Since all Brokers have messages, there is no need to Subscribe among ILDMs. This mechanism allows messages to be shared among Brokers, but since messages are broadcasted among ILDMs, the traffic among Brokers increased. Therefore, we introduce the Distributed MQTT broker by data Link lookup for Traffic reduction (DMLT) method, which adds routing control to this method to prevent duplicate messages.

III. PROPOSED METHOD, CALLED IS DMLT

A. ARCHITECTURAL DMLT

The DMLT method is intended to establish a route by using the Spanning Tree Protocol (STP), which is a data link layer protocol, for ILDM. The disadvantage of IP routing is that the network layer assigns an IP address to identify a peer, and the connection between devices is dependent on the IP address. Therefore, IP routing requires IP address information for DNS name resolution. IP operation at the network layer is not suitable for MQTT because it repeatedly processes connections from the data link layer to the application layer [12]. Spanning Tree Protocol (STP), a protocol at the data link layer, allows routing without IP addresses at the lower layers. An overview of DMLT is shown in Figure 3. DMLT communication sequence is shown in Figure 4. STP, a data link layer protocol, enables routing without IP addresses at the lower layers. STP provides blocking ports on the communication path to avoid loop configuration. Based on the DMLT mechanism, a port status message is specified to the ILDM. This allows the ILDM to investigate the blocking of a port using this message before the CONNECT message is forwarded (1). If the port is blocked, the CONNECT message is not forwarded. This reduces the number of connections between Brokers and duplication of messages. Therefore, the amount of traffic between Brokers can be reduced.

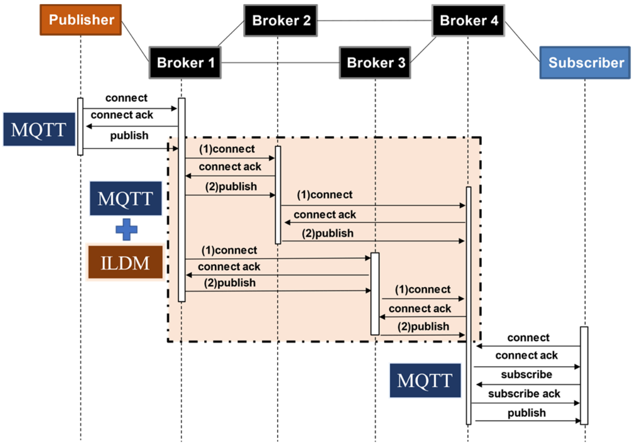


FIGURE 2. Communication sequence in ILDM mechanism.

B. PROTOTYPE

A diagram of the prototype DMLT system is shown in Figure 5.

MQTT communication uses Raspberry Pi as the device; the L2 switch is considered a Broker by connecting it to Raspberry Pi. The number of Brokers is a parameter in this study. 4 Layer2 (L2) switches and 4 Raspberry Pi are connected to the L2 switches, one Raspberry Pi in the role of Publisher and one in the role of Subscriber. The Broker runs on Raspberry Pi using Mosquitto [13]. A mesh network allows messages to be broadcast over the shortest path, even when the configuration is larger than that of a star or ring network. This reduces the number of times messages are routed, thereby reducing the amount of traffic [14]. Messages from the verification system are broadcasted using a system with a Proxy set up on a Raspberry Pi. The Broker with a Proxy shares messages with all Brokers and can respond

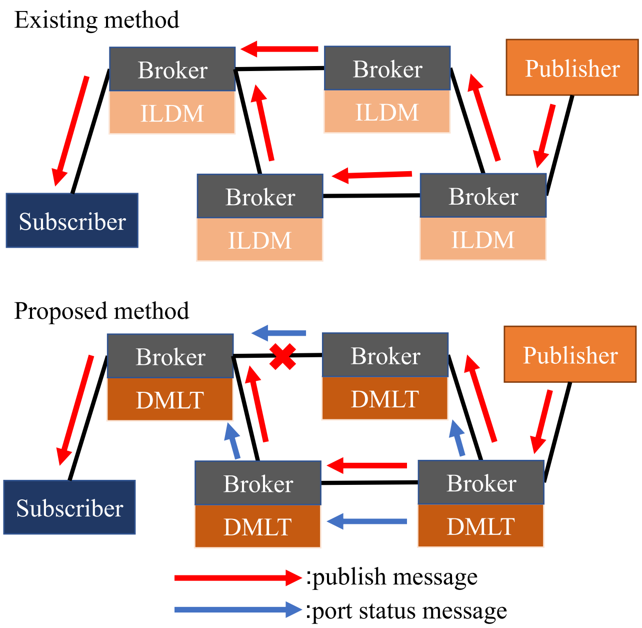


FIGURE 3. Overview of the DMLT.

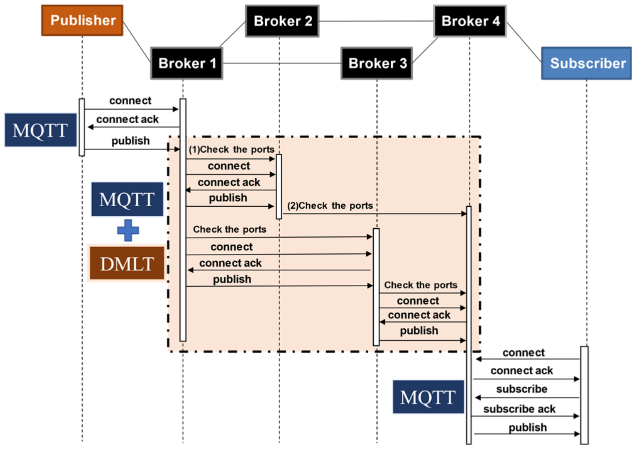


FIGURE 4. Communication sequence in DMLT mechanism.

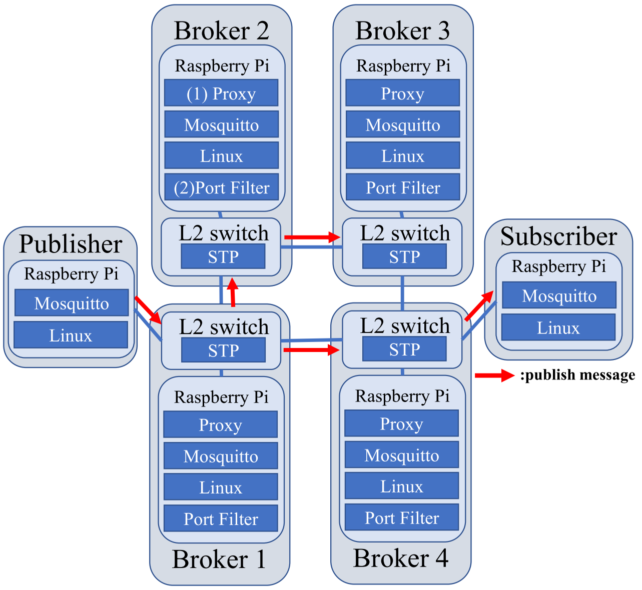


FIGURE 5. Diagram of the DMLT system.

immediately to a Topic requested by a Subscriber (Figure 5 (1)). The Broker that receives a message uses the identifier of the Broker that published it and the message as a hash value and records the time so that the same Broker does not receive the same message that was published. The Broker checks the port status of the L2 switch before sending a message. The status of the L2 switch next to the L2 switch to which the Raspberry Pi is connected must be checked as well. The status of the port on the L2 switch next to the L2 switch to which the Raspberry Pi is connected should be checked as well. This will help us select the port to send the data to (Figure 5 (2)).

C. SYSTEM CONFIGURATION EXPERIMENT

As an evaluation of the prototype, the average communication delay between Publisher Subscriber is measured when the number of brokers is changed from 2 to 6. The experimental configuration is shown in Figure 6. The Subscriber is connected to broker N when N brokers are used. The transmitted data was 128 [Byte].

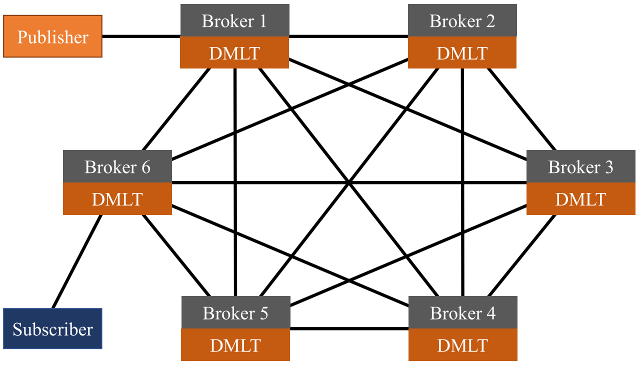


FIGURE 6. System configuration of performance evaluation.

The experimental results are shown in Figure 7. The figure shows that the communication delay time increases as the number of brokers increases. This is because the data is transferred to the connected brokers in turn, so it is thought that as the number of brokers increases, the communication delay time also increases.

D. PERFORMANCE EVALUATION

In this section, as a performance evaluation, traffic volumes are compared between DMLT and ILDM, one of the conventional methods. The experimental environment is shown in Figure 6. In the experiment, we compare the total traffic volume between Brokers when aggregating data sent from end devices. The data to be sent are 32, and 2048 [Bytes]. As a parameter, the number of Brokers is varied from 2 to 6. In Figure 6, the maximum environment configuration is six brokers. In the experiment, if N brokers are used, Broker 1 to Broker N are used. Subscriber connects

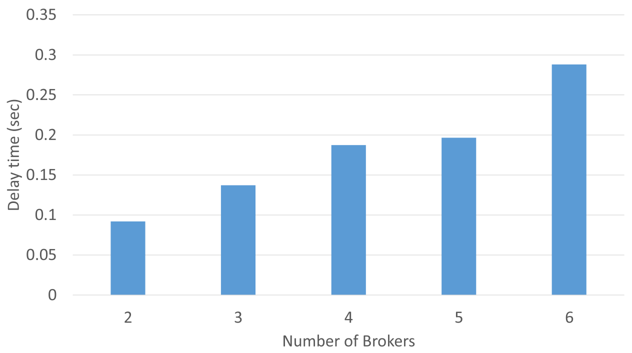


FIGURE 7. Average delay time of the proposed method.

to Broker N. Data communication is transmitted once per second on average at exponential distribution intervals. The aggregation time is one hour, and the average amount of traffic per second is compared. This experiment will monitor traffic using Wireshark. Figure 8 shows the experimental results. Figure 9 shows the amount of traffic reduced by DMLT. The results show that DMLT has less traffic than ILDM, the conventional method. In addition, this effect increases with the number of brokers. When the number of brokers is 6, it is found that the amount of traffic is reduced by about 66.7 %.

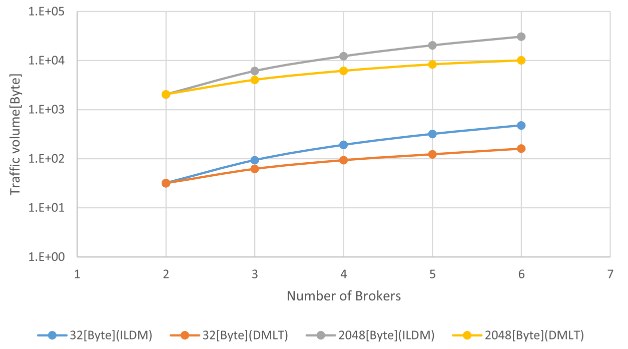


FIGURE 8. Comparison of traffic volumes between conventional and DMLT methods.

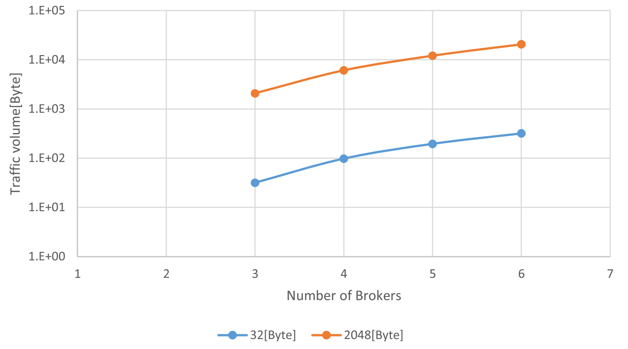


FIGURE 9. Traffic reduced by DMLT method.

IV. OVERVIEW OF WDMLT METHOD

A. ARCHITECTURE OF ROUTING WITH VPN & VLAN

The previous section described the DMLT method, which reduces the amount of traffic between distributed brokers. However, to operate distributed brokers in a real environment, there are cases where traffic over a wide area is aggregated, as shown in Figure 10. Therefore, the authors proposed a routing method that connects the locations. in actual operation, messages are controlled by a Layer 2-based routing mechanism within locations. For inter-broker cases, the connection is made using a VPN, and the destination of messages is fixed by VLANs. This routing mechanism is called the WDMLT method and is suitable for actual operation because VPNs can communicate across Network Address Translation (NAT) and firewalls. This approach uses IP as the destination address. For routing, VPNs [15] between locations and VLANs [16] between routers are used. In this approach, when external broker 1 receives a message, it connects to the external brokers in the other networks using a VPN; the VPN connects to each network via a router. The router configures VLANs and fixes connection points, such as Networks A and B. Afterwards, it connects with the broker via MQTT at a fixed connection point. The connected broker broadcasts messages to the external broker. This method requires IP control when using VLANs. However, compared to IP routing, this method is less IP-dependent. Also, because of static control, no new traffic is generated when additional locations are added [17]. Fault tolerance can be improved by setting up routes that switch automatically if a problem occurs with a route or node. However, routes are configured individually.

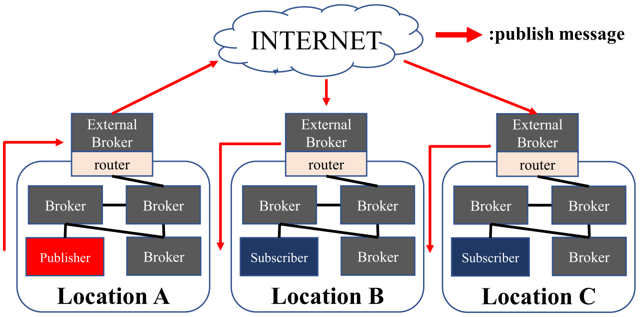


FIGURE 10. Overview of communications between locations.

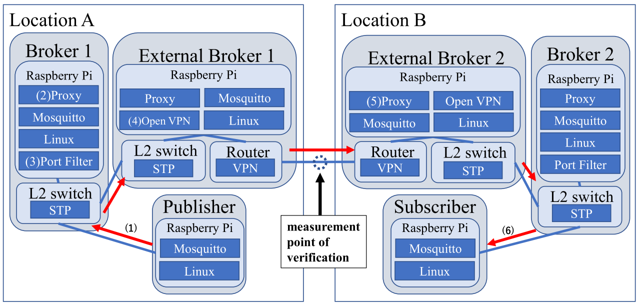
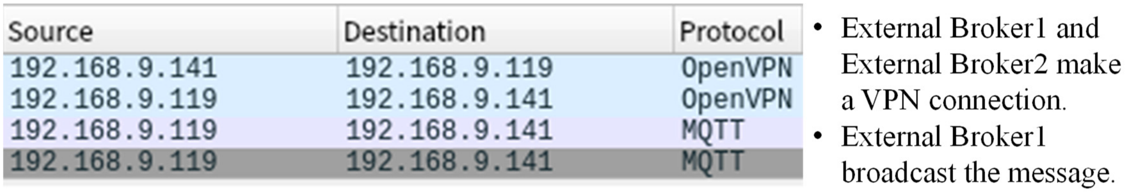


FIGURE 11. Experimental configuration of WDMLT method.

B. EXPERIMENT

The process of sending a message from Location A to Location B is described in Figure 11, which shows the experimental configuration for verifying the operation of



Source	Destination	Protocol
192.168.9.141	192.168.9.119	OpenVPN
192.168.9.119	192.168.9.141	OpenVPN
192.168.9.119	192.168.9.141	MQTT
192.168.9.119	192.168.9.141	MQTT

- External Broker1 and External Broker2 make a VPN connection.
- External Broker1 broadcast the message.

FIGURE 12. Verification screen at measurement point.

the WDMLT method. The following is a number-by-number description of the operation of each of the major WDMLT systems.

(1) Publisher sends a message to Broker1.

(2) Brokerage within a location is connected by Proxy.

(3) Broker1 investigates the port to which it is connected and checks to see if it is blocked.

(4) External Broker 1 connects to External Broker 2 via Open VPN when it receives a message.

(5) External Broker2 connects to Broker2 in the base via Proxy and broadcasts messages together.

(6) Broker2 sends a message to Subscriber when it receives a message.

In this way, the External Broker sends messages over the network. Next, the operation of the WDMLT system is verified in Figure 12. In this verification, Wireshark was used to collect packets. The top two lines are connection requests sent from External Broker1's private IP 192.168.9.141 to External Broke2's private IP 192.168.9.119. External Broke2 then replies with a response message. The bottom two lines show that after establishing the connection via VPN, External Broke1 makes the MQTT connection, and the message is sent. This indicates that the message was sent between the External Broker after the VPN connection was completed between the Router; the connection between the Publisher, Subscriber, and Broker was confirmed during the experiment with the DMLT method. From the above, it was confirmed that OpenVPN and MQTT are working.

V. ADAPTATION TO IoT DEP

A. OVERVIEW OF IoT DEP

Currently, communication platforms for the IoT is being discussed as a network for IoT communication [18], [19]. The IoT data exchange platform (IoT DEP) [20] is a communication platform that is a leading candidate for transport functionality. The IoT DEP has its architecture and requirements registered as an international standard in ISO/IEC JTC1/SC41 as ISO/IEC30161 series. In addition, the control method between Nodal Points is discussed in ISO/IEC 30161 Part 2.

B. ARCHITECTURE of IoT DEP

Figure 13 shows the concept of IoT DEP. The IoT DEP is that end devices and servers are accessed by Pub/Subtype communication, and the IoT DEP network consists of multiple Nodal Points that are connected by dedicated paths.

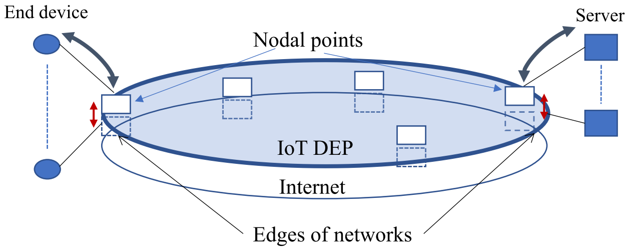


FIGURE 13. Concept of IoT DEP.

IoT DEP functions are implemented in Nodal Points. This allows many applications on the Internet to be connected to the IoT DEP network. MQTT is being considered as a communication protocol for use in IoT DEP. When using MQTT for IoT DEP, a distributed MQTT broker is required because the Nodal Point is the MQTT broker. Therefore, we adapt the method proposed in this paper.

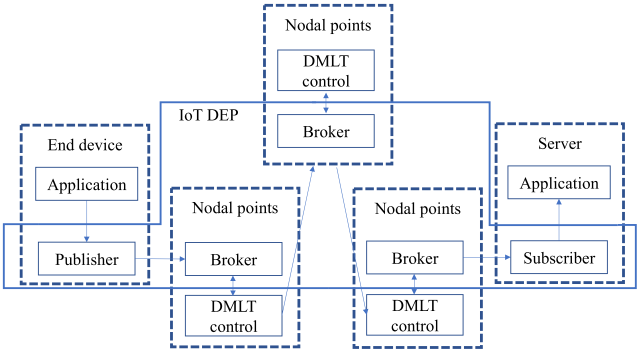


FIGURE 14. Relationship between the IoT DEP and the proposed mechanism.

C. APPLYING THE PROPOSED METHOD TO THE IoT DEP

The application of the control method proposed in this paper to IoT DEP is described below. The DMLT method applies to nodal point-to-point control shown in Figure 13. Figure 14 shows the case where data is sent from an end device to a Server. At the end device, data from the application is aggregated to the Broker of the connected Nodal points. When the data is transferred to the Broker of the Nodal point connected to the Server, the data is passed to the application through MQTT communication. The area framed in Figure 14 is the IoT DEP.

VI. CONCLUSION

In this study, the authors compared the performance of the DMLT method with conventional methods to evaluate its performance. The results showed that the DMLT method was more than twice as effective as the conventional method. We also proposed WDMLT, a control method that combines DMLT at local sites and the above methods between remote sites built a prototype of the WDMLT method, and confirmed its operation. Compared to the conventional method, these methods can be operated with lower traffic when sharing a large amount of IoT data.

REFERENCES

[1] *Information and Communication White Paper 2023 Edition*, Ministry Internal Affairs Commun., Tokyo, Japan, 2023.

[2] B. Wukkadada, K. Wankhede, R. Nambiar, and A. Nair, "Comparison with HTTP and MQTT in Internet of Things (IoT)," in *Proc. Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Jul. 2018, pp. 249–253.

[3] I. U. Din, H. Asmat, and M. Guizani, "A review of information centric network-based Internet of Things: Communication architectures, design issues, and research opportunities," *Multimedia Tools Appl.*, vol. 78, no. 21, pp. 30241–30256, Nov. 2019.

[4] M. B. Yassein, M. Q. Shatnawi, S. Aljwarneh, and R. Al-Hatmi, "Internet of Things: Survey and open issues of MQTT protocol," in *Proc. Int. Conf. Eng. MIS (ICEMIS)*, May 2017, pp. 1–6.

[5] R. Banno, J. Sun, S. Takeuchi, and K. Shudo, "Interworking layer of distributed MQTT brokers," *IEICE Trans. Inf. Syst.*, vol. E102.D, no. 12, pp. 2281–2294, 2019.

[6] Y. Noda, S. Ohno, K. Ishibashi, and T. Yokotani, "A new routing mechanism based on layer 2 control in MQTT networks with multiple brokers," *IEICE Commun. Exp.*, vol. 11, no. 6, pp. 307–312, 2022.

[7] N. Naik, "Choice of effective messaging protocols for IoT systems: MQTT, CoAP, AMQP and HTTP," in *Proc. IEEE Int. Syst. Eng. Symp. (ISSE)*, Oct. 2017, pp. 1–7.

[8] B. Mishra and A. Kertesz, "The use of MQTT in M2M and IoT systems: A survey," *IEEE Access*, vol. 8, pp. 201071–201086, 2020.

[9] T. Rausch, S. Nastic, and S. Dustdar, "EMMA: Distributed QoS-aware MQTT middleware for edge computing applications," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, Apr. 2018, pp. 191–197.

[10] J.-H. Park, H.-S. Kim, and W.-T. Kim, "DM-MQTT: An efficient MQTT based on SDN multicast for massive IoT communications," *Sensors*, vol. 18, no. 9, p. 3071, Sep. 2018.

[11] A. Al-Fuqaha, A. Khreishah, M. Guizani, A. Rayes, and M. Mohammadi, "Toward better horizontal integration among IoT services," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 72–79, Sep. 2015.

[12] Y. Sasaki, T. Yokotani, and H. Mukai, "Proposals on IoT communication through MQTT over L2 network and their performance evaluation," in *Proc. Int. Conf. Innov. Inf. Technol. (IIT)*, Nov. 2018, pp. 30–35.

[13] R. A. Light, "Mosquitto: Server and client implementation of the MQTT protocol," *J. Open Source Softw.*, vol. 2, no. 13, p. 265, May 2017.

[14] I. F. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Commun. Mag.*, vol. 43, no. 9, pp. S23–S30, Sep. 2005.

[15] R. Cohen, "On the establishment of an access VPN in broadband access networks," *IEEE Commun. Mag.*, vol. 41, no. 2, pp. 156–163, Feb. 2003.

[16] F. Shahriar and J. Fan, "Performance analysis of FHRP in a VLAN network with STP," in *Proc. IEEE 3rd Int. Conf. Electron. Technol. (ICET)*, May 2020, pp. 814–818.

[17] I. Kotuliak, P. Rybár, and P. Trúchly, "Performance comparison of IPsec and TLS based VPN technologies," in *Proc. 9th Int. Conf. Emerg. eLearn. Technol. Appl. (ICETA)*, Oct. 2011, pp. 217–221.

[18] J. Guth, U. Breitenbücher, M. Falkenthal, F. Leymann, and L. Reinfurt, "Comparison of IoT platform architectures: A field study based on a reference architecture," in *Proc. Cloudification Internet Things (CIoT)*, Nov. 2016, pp. 1–6.

[19] J. Guth, U. Breitenbücher, M. Falkenthal, P. Fremantle, O. Kopp, F. Leymann, and L. Reinfurt, "A detailed analysis of IoT platform architectures: Concepts, similarities, and differences," in *Internet of Everything*. Singapore: Springer, 2018, pp. 81–101.

[20] T. Yokotani and K. Kawai, "Concepts and requirements of IoT networks using IoT data exchange platform toward international standards," in *Proc. IEEE Conf. Standards Commun. Netw. (CSCN)*, Oct. 2019, pp. 1–6.

KAZUHIRO KOSAKA received the B.S. degree in electrical engineering and electronics from the Kanazawa Institute of Technology, in 2022, where he is currently pursuing the M.S. degree in electrical engineering and electronics. His research interests include the IoT networks and communication mechanisms. He is a Student Member of the IEICE.

YUTO NODA received the Graduate degree from the Department of Electrical and Electronic Engineering, Faculty of Engineering, Kanazawa Institute of Technology, in 2021, and the master's degree from the Kanazawa Institute of Technology, in 2023. He joined Mitsubishi Electric Information Network Corporation, in 2023.

TETSUYA YOKOTANI (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in information science from the Tokyo University of Science, in 1985, 1987, and 1997, respectively. He had worked for Mitsubishi Electric Corporation, in 1987, Since then, he has researched high-speed data communication, optical access systems, home network, and performance evaluation technologies of networks mainly with the Information Technology Research and Development Center. He moved to the Kanazawa Institute of Technology, in 2015. Since then, he has engaged research and education on networks for various IoT services. He has been the Chair of the IEEE ComSoc the CQR Technical Committee. Currently, he is the Chair of Advisory Board in this committee. He has also participated in the standardization activities on ITU-T SG15, SG20 and ISO/IEC JTC1. He is also a member of IEEE ComSoc and IPSJ, and a Fellow Member of IEICE.

KOICHI ISHIBASHI (Member, IEEE) received the B.S. and M.S. degrees from Osaka City University, in 1989 and 1991, respectively, and the Ph.D. degree in communications and integrated systems from the Tokyo Institute of Technology, in 2017. He joined the Mitsubishi Electric Corporation, in 1991. Since then, he has been engaged in research and development of internetworking equipment, mobile networking, and ad hoc network systems. Moreover, in 2019, he moved to the Kanazawa Institute of Technology as an Associate Professor. His current research interests include routing technologies for wireless sensor networks and the network architectures for IoT.