Regular Paper

A Proposal on New Control Mechanisms Based on ICN for Low Latency IoT Services

Atsuko Yokotani*, Hiroshi Mineno*, Satoshi Ohzahata** and Tetsuya Yokotani***

*Graduate School of Science and Technology, Shizuoka University, Japan

{yokotani.atsuko20@, mineno@inf.}shizuoka.ac.jp

**Graduate School of Informatics and Engineering, University of Electro-Communications, Japan
ohzahata@is.uec.ac.jp

***College of Engineering, Kanazawa Institute of Technology, Japan
yokotani@neptune.kanazawa-it.ac.jp

Abstract – Information Centric Network (ICN) is a promising candidate to mitigate protocol overheads on the Internet to transfer information. Currently, the Internet invokes Internet protocol (IP) address base routing and translation between the IP address and the indicator by the domain name system (DNS) to obtain information. In contrast, ICN obtains information directly and provides the networked cache function to reduce duplicate information transfer. In particular, these features provide advantages in Internet of Things (IoT) communication, including low latency services. Prioritized information should be transferred with low latency to users and should be shared with multiple users. For this purpose, it is proposed that networked cache provides dedicated space to store prioritized information. This paper describes detailed mechanisms on bandwidth reservation and networked cache functions and performance evaluation by network traffic emulation. This paper proposes an architecture referred to as "C-NAT" and mechanisms of ICN with traffic control functions (e.g., bandwidth reservation and cache control) and their performance evaluation. C-NAT is an abbreviation of "Content-centric network (CCN) with Network initiative And Traffic control" with some modifications of CCN, which is a typical mechanism in ICN technologies.

Keywords: IoT, ICN, Traffic control, Cache control, Low latency service

1 INTRODUCTION

The Internet of Things (IoT) is a worldwide topic of interest. As various services utilizing IoT are deployed, the communication network plays an important role. Most IoT services expect wide-area network services, including Internet services [1]. However, in the mature stage of IoT services, if these services are deployed over the Internet as it currently exists, some serious problems will be highlighted, e.g., large overheads of the legacy protocols, processing resources of their overhead in communication equipment, and processing power of Internet protocol (IP) address translation by the domain name system (DNS).

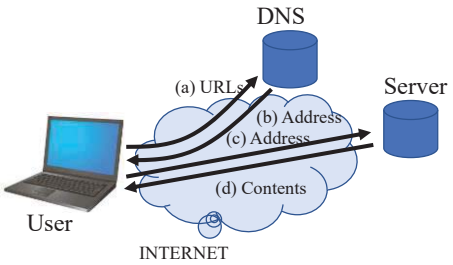
To mitigate these problems, Information-Centric Network (ICN) technologies have been discussed to facilitate IoT services. ICN technologies invoke independent communication of IP. They also provide networked cache to reduce duplicate traffic transfer.

This paper describes the possibilities of ICN technologies for IoT services and proposes architecture and operations of ICN base networks for various IoT services, referred to as "C-NAT" which is an abbreviation of "CCN with Network initiative And Traffic control." CCN is an abbreviation of "Content-Centric Network" and is summarized in the next section. Most significantly, this paper proposes operations with traffic control mechanisms with prioritized traffic flows on ICN base networks for low latency IoT services.

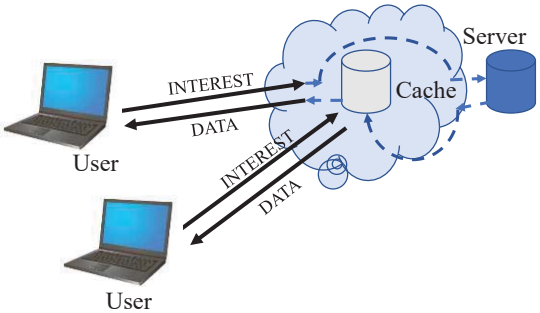
2 SURVEY ON ICN TECHNOLOGIES

ICN technologies include various mechanisms [2]. One typical mechanism is CCN proposed by [3]. CCN can provide simplified communication sequences to obtain information from servers. This paper focuses on CCN in ICN technologies.

Figure 1 compares sequences in the Internet and in CCN in the case of information transfer from a server to users.



Communication sequences in the Internet

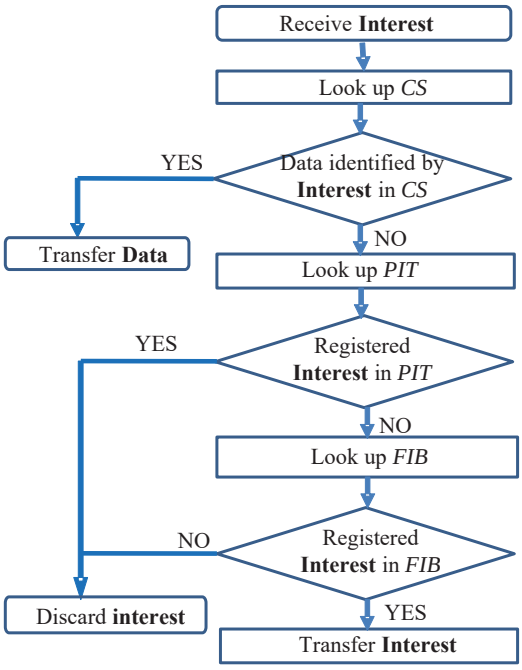


Communication sequences in CCN

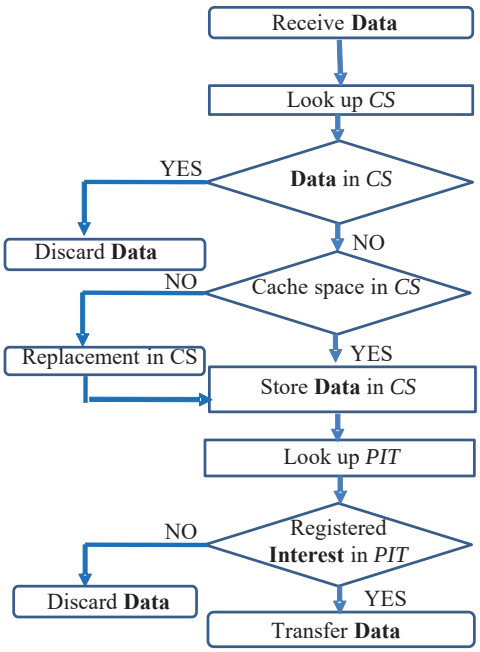
Figure 1 Comparison of communication sequences

With the Internet, before a user accesses a server to obtain particular content, the destination IP address must be derived from translation of a uniform resource locator (URL) by the DNS; see (a) and (b) in Fig. 1. Then, this user accesses the server using the derived IP address; see (c) in Fig. 1. As a result, this user obtains the requested content; see (d) in Fig. 1. In this case, because the user is connected to the server using these sequences, each user must invoke the same sequence whenever they access the server.

By implementing CCN, a user accesses the server using content names directly, without translation between an IP address and URL indicating the location of the content. Moreover, transferred content can be temporarily stored at some intervening, or interworking, points in networks. When another user accesses the server to obtain that content, the interworking point provides the requested content from its cache instead of the server. Therefore, duplicate transfer of contents by the server and the limited processing power of content transfer in the server are mitigated. In CCN, a request for content and the response, including the content, are referred to as **Interest** and **Data** messages, respectively. In this paper, these terms will reflect the same meaning. The detailed operations of CCN are described in Fig. 2. In CCN, there are three components to an Interworking point (IWP) (i.e., Content Store (CS), Pending Interest Table (PIT), and Forwarding Information Base (FIB)), which handle **Interest** and **Data**. IWPs are connecting points between CCN links and can be positioned as routers in the current Internet. Figure 2 (a) and (b) show processing sequences for **Interest** and **Data**, respectively.



(a) Processing sequences of **Interest**



(b) Processing sequences of **Data**

Figure 2 Processing sequences in CCN

3 COMMUNICATION SEQUENCES IN IOT SERVICES

To deploy IoT services, communication sequences are classified into three types, as shown in Fig. 3 [4]. Generally, an end device consists of various sensors, actuators and a communication device to connect a broadband network, e.g., high speed LAN, fiber to the X (FTTX), or radio access networks (RAN). Components in an end device are connected by wireless networks, e.g., LoRa and W-SUN, as a proximity network. The proximity network is relatively small and is configured for a dedicated purpose, so it can be optimized for specific services.

Of these, Type 1 seems to be in the majority because most IoT services require information from a large number of end devices, including sensors as end points of communication. In these sequences, some interworking points relay information of IoT services.

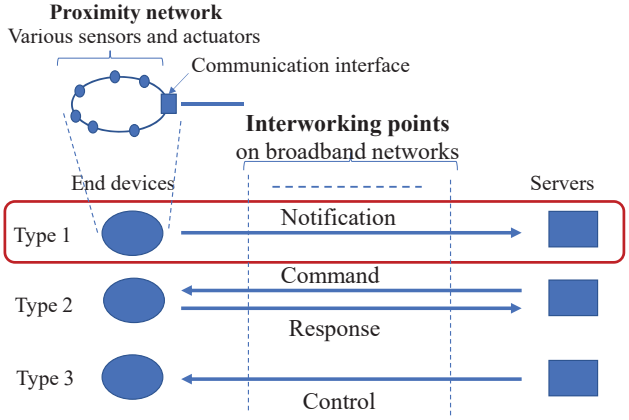


Figure 3 Types for IoT services in communication sequences

The studies on IoT services based on ICN technologies, especially CCN, have been published in previous research, e.g., [5] and [6]. Moreover, these studies have been discussed by the ICN Research Group of the Internet Research Task Force (IRTF) [7] as one of the next standardized subjects.

In common agreement in these studies, when ICN technologies are applied to IoT services, these technologies provide simpler communication for IoT services than conventional Internet technologies. For example, in IoT services, the huge number of end devices create tiny information blocks and transfer these blocks across networks, e.g., Type 1 in Fig. 3. In this situation, large protocol headers, i.e., the hypertext transfer protocol (HTTP), and three-way handshake procedures in transmission control protocol and IP (TCP/IP) cause an increase in traffic volume. Moreover, processing in DNS generates a heavy load for communication equipment.

ICN technologies are designed to mitigate these problems in deployment of IoT service. However, ICN may cause a security issue. Especially in the case of Type 1 of Fig. 3, when suspicious devices are connected to networks, distributed denial of service (DDoS) attacks may be initiated. This problem has been indicated in [8]. In that paper, authors proposed that an interworking point in networks could provide a screen of transfer traffic prior to endpoints as one of the regulation mechanisms on incoming IoT traffic, as shown in Fig. 3.

Generally, in the case of Type 1, end devices transfer information periodically to networks. In particular, real-time services in IoT will require periodic transfer sequences [9]. Requirements of these services are surveyed in [9] as described in Table 1. These services are typical examples. In addition to these, services categorized as Ultra-Reliable and Low Latency Communications (URLLC), a type of services in the 5G mobile system, have the same characteristics [10].

Generally, these services invoke memory-to-memory communications [11]. Each server includes the Shard memory to receive information from end points as shown in Fig. 4. The update of each field is cyclically invoked according to service requirements. The update cycle includes the transfer and processing delay. For instance, when this cycle is small, the transfer delay will be small. Therefore, information is transferred using multiple priorities in the network. This approach has been applied to low-latency communication systems in the industrial field, e.g., [12] and [13].

Table 1 Summary of QoS requirements of IoT services with low latency

	Latency (ms)	Packet loss ratio	Cycle (ms)	Size (B)	Device density
Factory	0.25～10	10^{-9}	0.5～50	10～500	0.33～3/m^3
Industrial plant	50～100	10^{-4}～10^{-3}	100～5000	40～100	10000 /Plant
Smart grid	3～20	10^{-6}	10～100	80～1000	10～2000/km^2
Transportation (Safety drive)	10～100	10^{-5}～10^{-3}	100～1000	～1000	500～3000/km^2

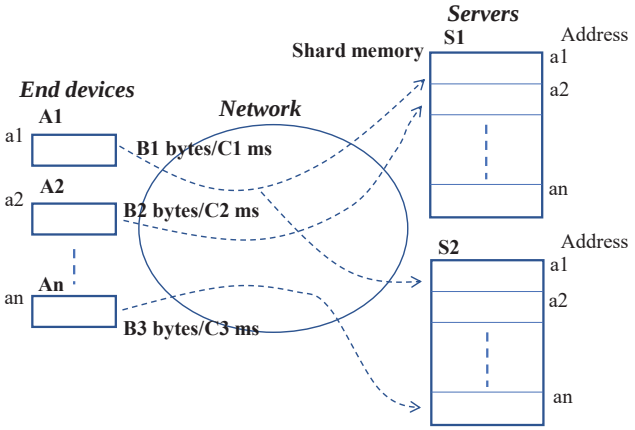


Figure 4 Examples of information transfer between end devices and servers

In Fig. 4, End devices A1, A2, … and An cyclically transfer information to Servers S1 and S2 across a network. Information is saved in the Shard memory in each Servers. In this case, the area in the Shard memory and the update cycle are allocated according to the service requirements. In this figure, B2 byes of information are shared from End device A2 to Sever S1 and updated every C2 ms. The network must comply with these conditions using traffic control functions with multiple priority levels.

4 PROPOSED MECHANISMS OF ICN WITH TRAFFIC CONTROL

In Section 3, the possibilities and new issues of IoT services based on ICN technologies were described. However, ICN technologies for IoT services do not provide traffic control functions. Generally, IoT services are overlaid across ICN base networks. In this situation, some traffic functionalities should be provided to improve the quality of service (QoS). In this section, the authors propose an architecture for new data transfer based on CCN with traffic control functions, referred to as “C-NAT”, and detailed mechanisms according to this architecture. In this paper, mechanisms with traffic control functions focusing on reservation of bandwidth and priority control in cache are proposed.

4.1 Architecture of C-NAT

In C-NAT, triggers for information transfer are provided by the IWP accommodating end devices, although end devices initiate information transfer by **Interest** in CCN. Because low latency IoT services invoke periodic information transfer as described in the previous section, the IWP can provide these triggers. The conceptual operations are shown in Fig. 5. In this figure, if information transfer is performed in less than half the cycle period identified in Table 1, the cycle time in Table 1 is guaranteed.

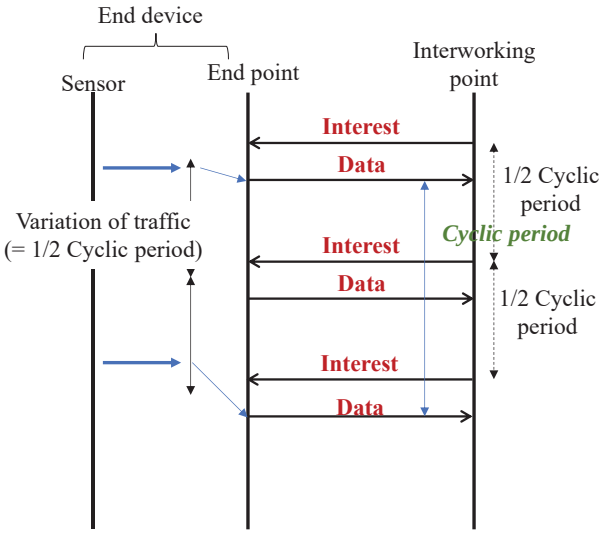


Figure 5 Conceptual operations in C-NAT

These operations are useful for the Type 1 communication sequence in Fig. 3. They also protect the network from DDoS attacks. However, information relay among multiple IWPs and traffic control on relayed routes should be specified. These points are specified in the subsequent sub-sections.

4.2 Information Relay Mechanisms for IoT Services

Information relay mechanisms based on CCN are shown in Fig. 6.

In Fig. 6, end devices are deployed according to offered services, e.g., monitoring of industry plants. At first, Server #1 submits an **Interest** to obtain information through some Interworking points (IWPs). Then, end devices reply to Server #1 with **Data** containing target information. After that, IWP #1 transfers that **Interest** periodically according to provisioning timing, e.g., required cycles. As the PIT in each IWP is set after the first **Interest**, **Data** is transferred to each IWP and can be stored in cache (Content Store) for every periodic **Interest**.

If other servers, e.g., Server #2, intend to obtain information regarding the **Interest**, IWP #3 updates the PIT to indicate requested information by a new server and then provides the **Data** stored in cache.

The processing sequences of **Interest** at IWP, which accommodates End devices, i.e., IWP #1 shown in Fig. 5, should be modified as in Fig. 7(a). The processing sequences of **Data** at the IWP, which relays **Data**, i.e., IWP #2 shown in Fig. 7(b), should be added to the original sequence. Other sequences are compiled in the original sequence shown in Fig. 2.

Sequences shown in these figures are clarified as follows. In Fig. 7(a), the first access to obtain information is the same as the original sequence. In short, the server generates **Interest** to end device. At this time, PIT was already set in IWP #1. In the second access and after, **Interest** to end devices is generated periodically according to provisioning timing, which is preset based on the required cycle in each service. In Fig. 7(b), IWP #2 monitors receiving **Data** periodically. If **Data** is not received, PIT is reset in IWP #2 automatically.

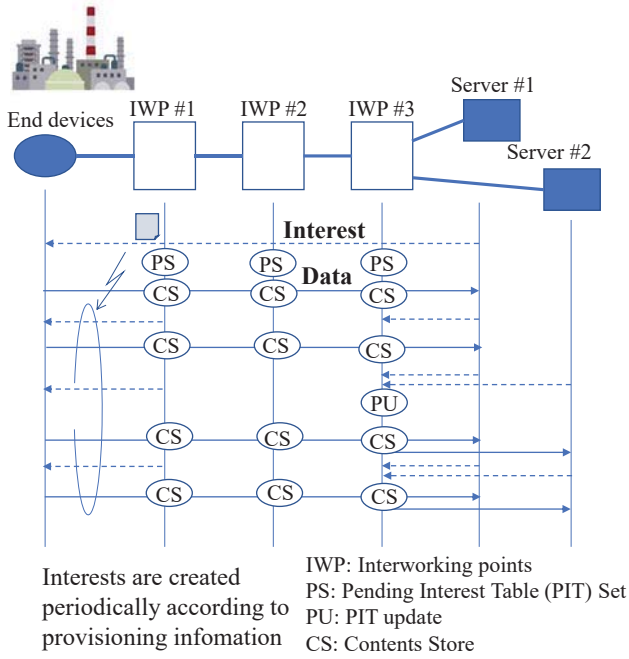
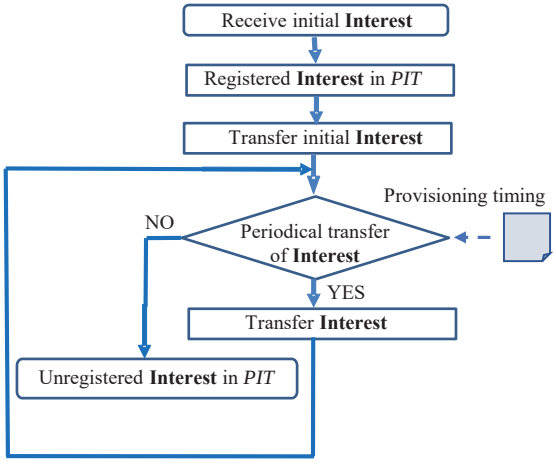
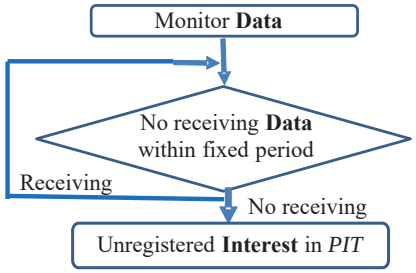


Figure 6 Operations in basic transfer mechanisms



(a) Processing sequences of **Interest** in IWP #1



(b) Additional processing sequences of **Data** in IWP #2

Figure 7 Detailed operations in proposed mechanisms

In these mechanisms, triggers to transfer information are provided by the IWPs. Therefore, DDoS attacks initiated from end devices cannot be successful. Moreover, these mechanisms do not increase traffic volume by taking advantage of ICN technologies.

4.3 Mechanisms with Traffic Control

In Section 4.1, basic transfer mechanisms were proposed. However, when services are aggregated on networks, traffic control functions should be provided to prioritize IoT services requiring low latency. For this purpose, bandwidth reservation and dedicated space in the cache of IWPs are proposed.

A summary of these proposed mechanisms is shown in Fig. 8. Multiple QoS requirements are specified in this system as described in Section 3. Transferred information can be classified into multiple priority levels according to the delay and/or loss requirements. It is important to note that priority control is operational issues and does not majorly impact cost of these IoT services.

In this section, mechanisms on two-priority level are described, e.g., prioritized and non-prioritized information.

Before information is transferred, priority levels should be provisioned. Then, priority levels can be recognized by attributes in **Interest** and **Data**. Each Interest and Data is transferred according to their indicated priorities across networks.

(1) Bandwidth reservation and priority control

In Fig. 8, each link has guaranteed bandwidth for prioritized information, which consists of an **Interest** and **Data** pair. In this system, prioritized information can utilize the full capacity if non-prioritized information is not transferred. In each IWP, dedicated cache space is assigned for prioritized **Data**. With these traffic control functions, guaranteed bandwidth is reserved by the dual leaky bucket mechanism [14]. The bandwidth less than the commitment information rate (CIR) should be reserved for prioritized information. The bandwidth of more than the CIR and less than the sustainable information rate (SIR), e.g., link rate, can be reserved for prioritized information according to availability of non-prioritized information. Moreover, at each IWP, prioritized information is transferred prior to non-prioritized information according to head of the line (HoL) scheduling [15].

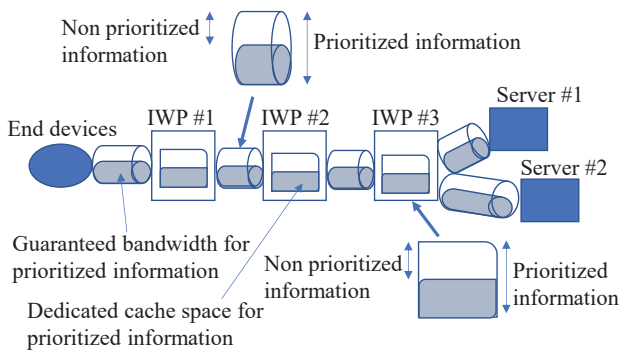


Figure 8 Traffic control functions in networks

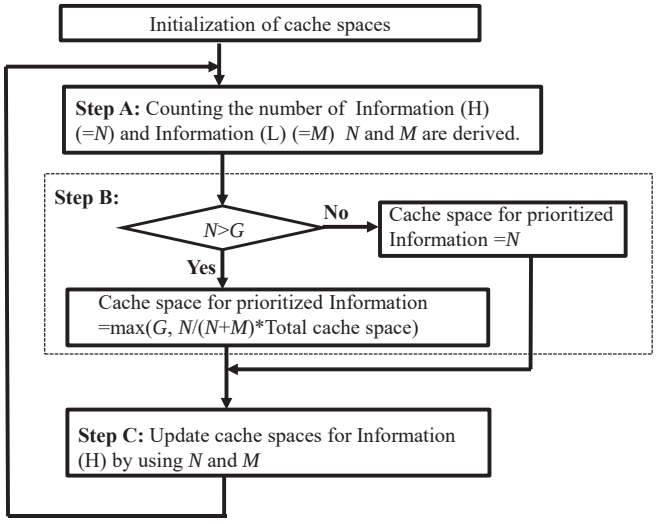


Figure 9 Cache control mechanisms for dedicated space

(2) Cache control

With cache control function, cache control mechanisms have been discussed in many articles. Control of dedicated cache space for prioritized information is provided as follows. Typical control mechanisms are the Least Recent Used (LRU), Least Frequency Used (LFU), and their combined mechanism [16].

As a legacy cache control, LRU is a policy under which stored information with the longest elapsed time after the last access is replaced when there is a shortage of cache space. LFU is a policy under which stored information with the smallest access frequency is removed from the cache space first. Prioritized information is always stored in cache spaces under this policy. Therefore, latency of prioritized information can be reduced [17]. However, these methods just relatively assign priority of information [18] and do not always guarantee communication quality of information transfer.

Authors have promoted new cache control mechanisms to improve these conventional mechanisms by utilizing real-time incoming information [19]. In this paper, these mechanisms are enhanced to adopt IoT communications. Essentially, full cache space can be assigned for prioritized information if non-prioritized information is not stored in cache as shown in Fig. 8. The proposed mechanism on control of dedicated cache space specifies the following operations.

In Fig. 9, each IWP counts incoming information within a fixed interval (Step A in Fig. 7). The numbers of information, prioritized and non-prioritized, are indicated by N and M, respectively. The volume of dedicated space for prioritized information is indicated by G. If N is larger than G, cache space for prioritized information is updated according to Equation (1). Otherwise, N is assigned to its space (Step B in Fig. 9).

$$\text{Cache space for prioritized information} = \max\left\{G, \frac{N}{N+M} \times Total\ cache\ space\right\} \quad (1)$$

Then, dedicated cache space is updated periodically (Step C in Fig. 9).

5 PERFORMANCE EVALUATION

In this section, the proposed mechanisms are evaluated using the CCN software platform referred to as CCNx [20].

5.1 Network Configuration

Two network configurations for performance evaluation are shown in Figs. 10 and 11. In Fig. 10, an IWP connects end devices and eight servers. The two servers processed prioritized information. Other servers processed non-prioritized information. Therefore, in the link between end devices and the IWP, bandwidth was reserved for prioritized information. This configuration corresponds to the small-scale deployment, e.g., IoT services across LAN. For example, various information generated from sensors in a site is monitored by several services specified by every service. This case referred to as the Local deployment case.

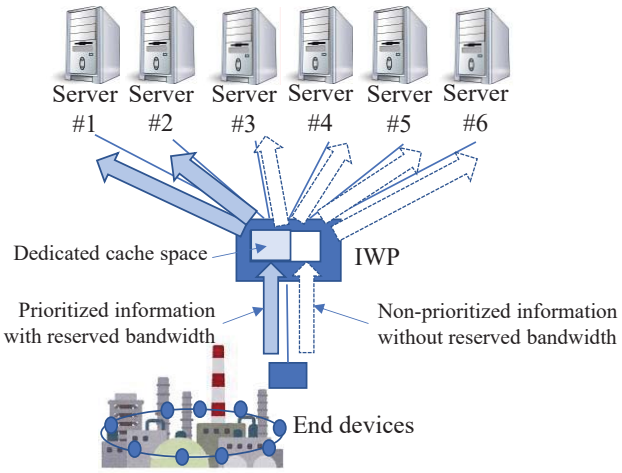


Figure 10 Network configuration with one IWP

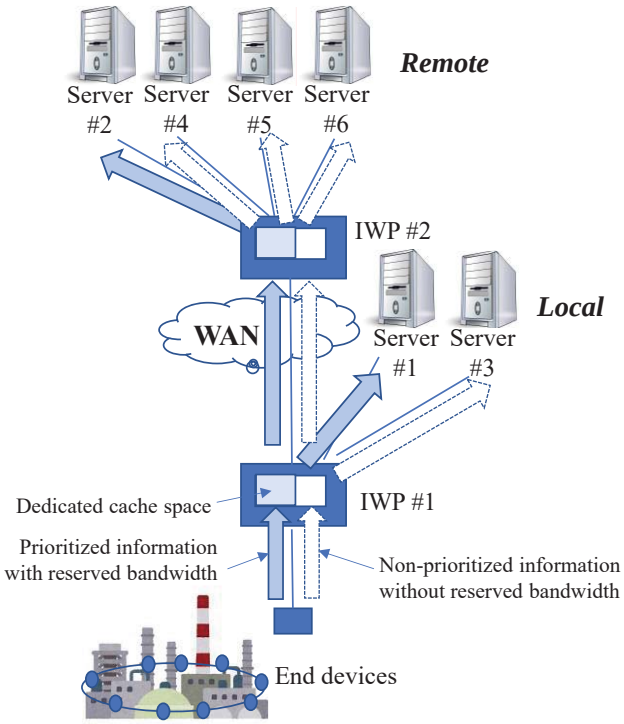


Figure 11 Network configuration with two IWPs

In Fig. 11, two IWPs were deployed in the system. IWP #1 connected two servers: one server for prioritized information and one for non-prioritized information. It also connected IWP #2. IWP #2 connected four servers. Three servers (Servers #4–#6) processed non-prioritized information. Server #2 processed prioritized information. In the links between end devices and IWP #1 and between IWP #1 and IWP #2, bandwidth was reserved for prioritized information. In IWPs #1 and #2, dedicated cache space was provided for prioritized information. This configuration corresponds to the Local-Remote deployment case, e.g., IoT services across WAN and LAN. WAN, e.g., the Internet or dedicated networks, is deployed between IWP #1 and IWP #2. IWP #1 is located at the nearby area of end devices. Servers accommodated in IWP #1 locally monitor information generated from end devices. On the other hand, Servers accommodated in IWP #2 remotely monitor such information.

In these configurations end devices, servers, and IWPs were emulated using Linux PCs with CCNx.

5.2 Numerical Examples

In this performance evaluation, bandwidth was denoted by the number of "unit" which is a virtual time on PC because CPU in PCs cannot emulate a real bit rate. Parameters from the performance evaluation were as follows:

- Link rate (=SIR) 10 Mb/unit
- Reserved bandwidth (=CIR) 3 Mb/unit
- Information block size 4 kB
- Generating rate of Interest for Prioritized information 50/unit

- Generating rate of Interest for non-Prioritized information 50/unit
- Dedicated space of cache 1500
- Total space of cache 4500
- Update cycle of dedicated space 1 unit
- Basic policy of cache LRU

In these parameters, “unit” is the unit of virtual time on the PC.

Some numerical results are shown in Figs. 12–15. In these graphs, the vertical axis denotes the latency in “unit” in the parameter list.

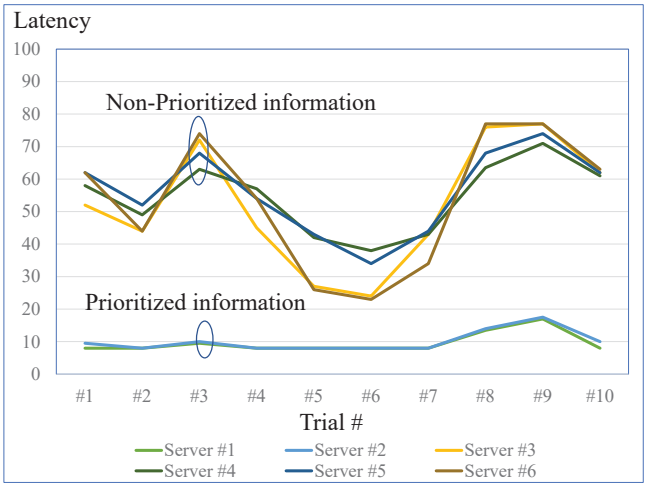


Figure 12 One IWP with cache control

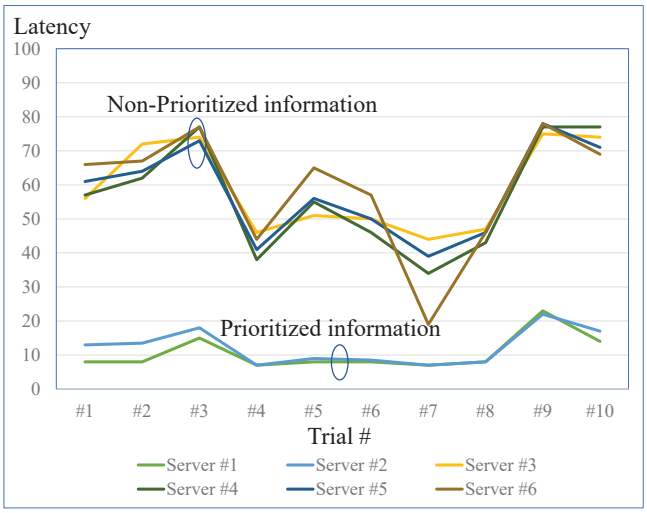


Figure 13 One IWP without cache control

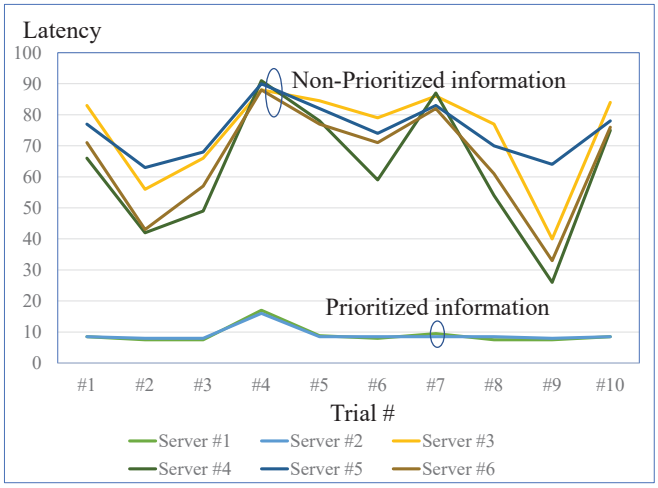


Figure 14 Two IWPs with cache control

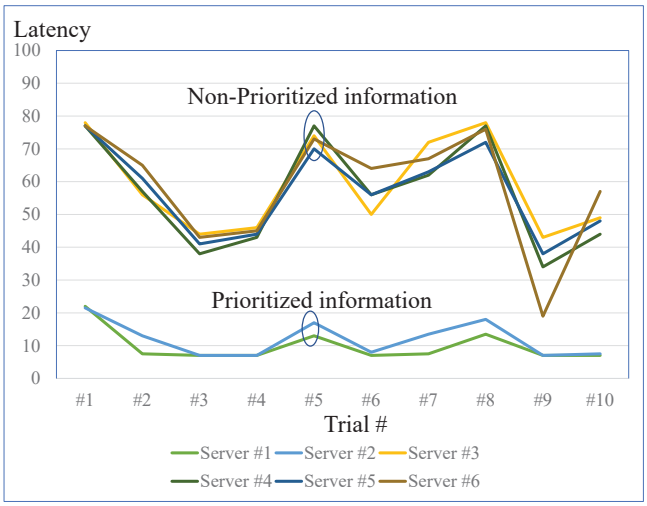


Figure 15 Two IWPs without cache control

These graphs show latency between **Interest** and **Data** in each server. The number of trials was 10 for each condition, as shown in the horizontal axes. The vertical axes show the latency by relative values. It is indicated as Latency denoted by “unit”.

In these cases, bandwidth reservation for prioritized information was always activated. Cache control by assignment of dedicated space for prioritized information was activated in the cases displayed in Figs. 12 and 14. It was not activated in the experimental cases of Figs. 13 and 15.

The delay of prioritized information is relatively smaller than the delay of non-prioritized information regardless of cache conditions, i.e., with or without cache. However, behaviors of prioritized information with cache control seem to be more stable than the case of without cache.

Moreover, when the two IWPs case is compared with the one IWP case, delay of prioritized information with cache control is almost the same. It can be concluded that delay of prioritized information is relatively stable independent of the system scale if cache control is activated.

The results indicate that the latency of non-prioritized information is three or four times of prioritized information. In this evaluation, the latency was modelled using virtual

time. However, because the propagation delay among transmission links can be negligible, these characteristics are applicable at the real time scale, e.g., millisecond and microsecond orders.

To confirm these characteristics, as characteristics of these examples are highlighted, the confidence interval with 95% in each case is shown in Figs. 16 and 17. In Fig. 17, differential of delay between servers accommodated in IWP #1 and in IWP #2 is small. Especially, in the cache control case, the characteristics of Server #1 and Server #2 are almost the same. Moreover, it is verified that prioritized information exhibits lower latency variation than that exhibited by non-prioritized information. When cache control is activated in each server, the variation in the latency of prioritized information is much smaller than that observed cache control activation. Restricting latency variation is one of important issues in low latency services, especially, industry fields. Hence, it can be concluded that the proposed mechanisms are reasonable.

Therefore, even in the Local-Remote deployment, the delay of prioritized information with cache control can be maintained in low latency except for propagation delay across networks.

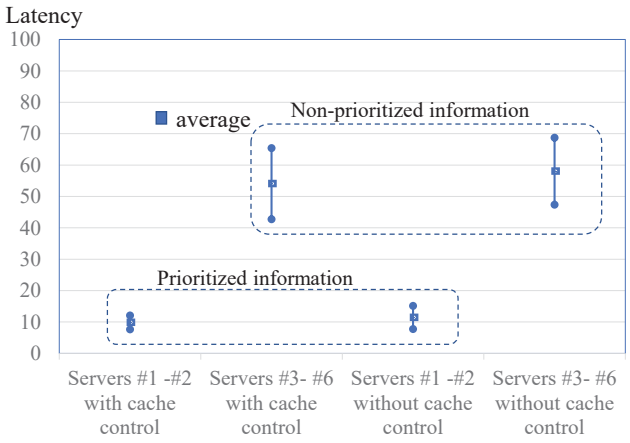


Figure 16 The 95% confidence interval in one IWP

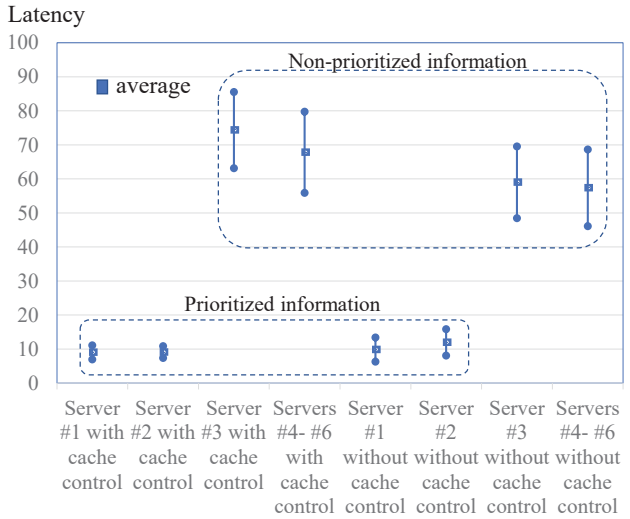


Figure 17 The 95% confidence interval in two IWPs

Performance evaluation can be summarized as follows.

Through these numerical examples, bandwidth reservation and cache control were confirmed effective for transfer of prioritized information including the Local-Remote deployment case. Especially, bandwidth reservation contributed to a reduction of latency. Moreover, cache control provided smaller variation of latency for prioritized information.

6 CONCLUSIONS

This paper proposed transfer mechanisms in IoT communication using ICN technologies. ICN technologies can solve communication problems of IoT presented by the current Internet and provide some advantages in IoT communication. However, security issues, e.g., DDoS attack, must be considered. This paper proposed communication sequences based on CCN to solve this issue.

Moreover, to comply with low latency requirements of IoT services, we proposed traffic control functions, including bandwidth reservation and cache control. Finally, this paper confirmed the advantages of the proposed mechanisms by the emulated system.

Currently, the IoT communication platform is an attractive topic for large-scale deployment. Standard development organizations (SDOs) are addressing this topic. For example, ISO/IEC JTC1/SC41 for IoT and digital twin has promoted this topic [21]. Proposals in this paper will contribute to this activity as detailed mechanisms in the IoT Data Exchange Platform (IoT-DEP), ISO/IEC 30161 series, which are summarized in [1].

REFERENCES

[1] T. Yokotani, and K. Kawai, “Concepts and requirements of IoT networks using IoT Data Exchange Platform toward International standards”, IEEE Conference on Standards for Communications and Networking (IEEE CSCN), #1570570960 (2019), DOI: 10.1109/CSCN.2019.8931337, IEEE Xplore.

[2] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher and B. Ohlman, “A survey of information-centric networking”, IEEE Communication Magazine, pp. 26-36, Vol. 50, Issue 7 (2012).

[3] V. Jacobson, D. K. Smetters, J. D. Thornton, M. Plass, N. Briggs and R. Braynard, “Networking Named Content,” ACM CoNEXT 2009, pp.1-12 (2009).

[4] T. Yokotani, S. Yamamoto, S. Ohno, K. Sasabayashi and K. Ishibashi, “Survey and comparison of Interworking point routing mechanisms for IoT services in wide area ICNs”, International Conference on Emerging Technologies for Communications (ICETC 2020), D2-4, (2020).

[5] 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 and Applications, vol. 78, pp. 30241–30256 (2019).

[6] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, “Information-centric networking for the internet of things: challenges and opportunities”, IEEE Network, vol. 30, no. 2, pp. 92-100 (2016).
[7] R. Ravindran, Y. Zhang, L. A. Grieco, A. Lindgren, J. Burke, B. Ahlgren and A. Azgin, “Design Considerations for Applying ICN to IoT”, ICNRG, Technical report, draft-irtf-icnrg-icniot-03, https://datatracker.ietf.org/doc/draft-irtf-icnrg-icniot/ (2018).
[8] A. Yokotani, H. Mineno and T. Yokotani, “A proposal on the access control mechanism for real time IoT services using ICN technology”, IoT Enabling Sensing/Network/AI and Photonics Conference 2021 (IoT-SNAP 2021), IoT-SNAP-5-06 (2021).
[9] P. Schulz, M. Matthe, H. Klessig, M. Simsek, G. Fettweis, J. Ansari, S. A. Ashraf, B. Almeroth, J Voigt, I. Riedel, A. Puschmann, A. Mitschele-Thiel, M. Muller, T. Elste and M. Windisch, “Latency critical IoT applications in 5G: Perspective on the design of radio interface and network architecture”, pp. 70-78, IEEE Communication Magazine, February (2017).
[10] G. A. Akpakwu, B. J. Silva and G. P. Hancke, “A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges”, pp. 3619 – 3647, Vol. 6, IEEE Access (2018).
[11] D. Buntinas, G. Mercier and W. Gropp, "Implementation and evaluation of shared-memory communication and synchronization operations in MPICH2 using the Nemesis communication subsystem", Journal of Parallel Computing, Vol. 33, No. 9, pp. 634-644 (2007).
[12] K. Oya, K. Tanaka, T. Sato, M. Yoshida and N. Todoroki, “Communication Method of Ring Network for Industrial System”, C-015, Forum on Information Technology 2018 (FIT 2018) (2018).
[13] P. Danielis, J. Skodzik, V. Altmann, E. B. Schweissguth and F. Golatowski, D. Timmermann and J. Schacht, “Survey on Real-Time Communication Via Ethernet in Industrial Automation Environment”, PF-000167, 19th IEEE International Conference on Emerging Technologies and Factory Automation (IEEE ETFA 2014) (2014)
[14] S. Zeng, N. Uzun and S. Papavassiliou, “A dual level leaky bucket traffic shaper architecture for DiffServ networks”, 2001 IEEE Workshop on High Performance Switching and Routing (HSPR 2001) (2001), DOI: 10.1109/HPSR.2001.923607, IEEE Xplore.
[15] T. Maertens , J. Walraevens, H. Bruneel, “A modified HOL priority scheduling discipline: Performance analysis”, European Journal of Operational Research, Vol. 108, pp. 1168-1185 (2007).
[16] H. Li, H. Nakazato, A. Detti, Nicola and B. Melazzi, "Popularity Proportional Cache Size Allocation Policy for Video Delivery on CCN", European Conference on Networks and Communications (EuCNC 2015), pp. 434-438 (2015).
[17] S. Jihoon, R. June-Koo Kevin and J. Sangsu, "Lightweight caching strategy for wireless content delivery networks", IEICE Communications Express, Vol. 3, No. 4, pp. 150-155 (2014).
[18] H. Qian, W. Muqing, H. Hailong, W. Ning and Z. Chaoyi, "In-Network Cache Management Based on Differentiated Service for Information-Centric Networking", IEICE Transactions on Communications, Vol.E97-B, No.12, pp. 2616-2626 (2014).
[19] A. Yokotani, S. Ohzahata, R. Yamamoto and T. Kato, “A Dynamic Cache Size Assignment Method with Bandwidth Reservation for CCN”, 2019 International Conference on Information Networking (ICOIN 2019), P2-15 (2019), DOI: 10.1109/ICOIN.2019.8718174, IEEE Xplore.
[20] "CCNx project”, http://www.ccnx.org.
[21] T. Yokotani, and K. Kawai, “Survey on standardization activities of IoT and proposal of the IoT data exchange platform”, International Conference on Emerging Technologies for Communications (ICETC 2020), IB3-3 (2020).

(Received: October 30, 2021)
(Accepted: September 5, 2022)

Atsuko Yokotani received BE, ME in Tokyo University of Technology and The University of Electro-Communication in 2017, 2019, respectively. Since then, she has joined Mitsubishi Electric Corporation. Currently, she engages development on control networks for self-defense system in Kamakura works. She has been also a doctoral course student in Graduate school of Science and Technology, Shizuoka University from 2020. She obtained an industry paper award in IWIN 2021. She is a member of IEICE.

Hiroshi Mineno received his B.E. and M.E. degrees from Shizuoka University, Japan in 1997 and 1999, respectively. In 2006, he received his Ph.D. degree in information science and electrical engineering from Kyushu University, Japan. Between 1999 and 2002, he was a researcher in the NTT Service Integration Laboratories. In 2002, he joined the Department of Computer Science of Shizuoka University as an Assistant Professor. He is currently a Professor. His research interests include Intelligent IoT systems as well as heterogeneous network convergence. He is a senior member of IEEE, IEICE and IPSJ, a member of ACM and the Informatics Society.

Satoshi Ohzahata received the B.S., M.E., and D.E. degrees from the University of Tsukuba, Ibaraki, Japan, in 1998, 2000, and 2003, respectively. From 2003 to 2007 and from 2007 to 2009, he was a Research Associate in the Department of Computer, Information and Communication Sciences and an Assistant Professor, respectively, at Tokyo University Agriculture and Technology. Since 2009, he has been an Associate Professor at the University of Electro-Communications, Tokyo, Japan. His interests are mobile ad hoc networks, the Internet architecture in mobile environments, and Internet traffic measurement. Dr. Ohzahata is a member of IEEE, ACM, IEICE and IPSJ.

Tetsuya Yokotani received B.S., M.S, and Ph.D. degrees on information science from the Tokyo University of Science in 1985, 1987, and 1997, respectively. He joined the 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 in the Information Technology R&D Center. In 2015, he moved to the Kanazawa Institute of Technology as a professor of College of engineering. Since then, he has engaged research and education on networks for various IoT services and has proposed standardization in these related areas. Currently, he is a chair in the IEEE ComSoc the CQR technical committee and a chair-elect in the Hokuriku branch of IEICE. He has also participated in the standardization activities on ITU-T SG15, SG20 and ISO/IEC JTC1 and obtained several awards on these activities. He is a fellow member of IEICE. He is also a member of IEEE ComSoc and IPSJ.