Multicast Technology for Broadcast-type Data Delivery Services

Hidetoshi Ueno[†]*, Hideharu Suzuki, Kiyoko Tanaka, and Norihiro Ishikawa*

Abstract

With the evolution of 3G (third generation) broadband mobile communication networks and the growing demand for multimedia applications, multicasting is gaining popularity as a key technology for broadcast-type data delivery services. We have developed protocol techniques for reliable multicast, multicast security, and multicast session management.

1. Introduction

In recent years, multicasting has come back into favor as a technique for implementing broadcast-type communication in mobile communication networks. Multicasting is a technique for delivering data to only the requesting clients whereas broadcasting delivers data to all clients simultaneously. Compared with unicasting, where data is transmitted to a specific receiver by designating a single address within the network, multicasting provides an efficient means of transmitting data across networks (**Fig. 1**). It is especially effective in mobile communication networks where available radio resources are limited.

Internet protocol (IP) multicasting is a technique for implementing multicasting on IP networks like

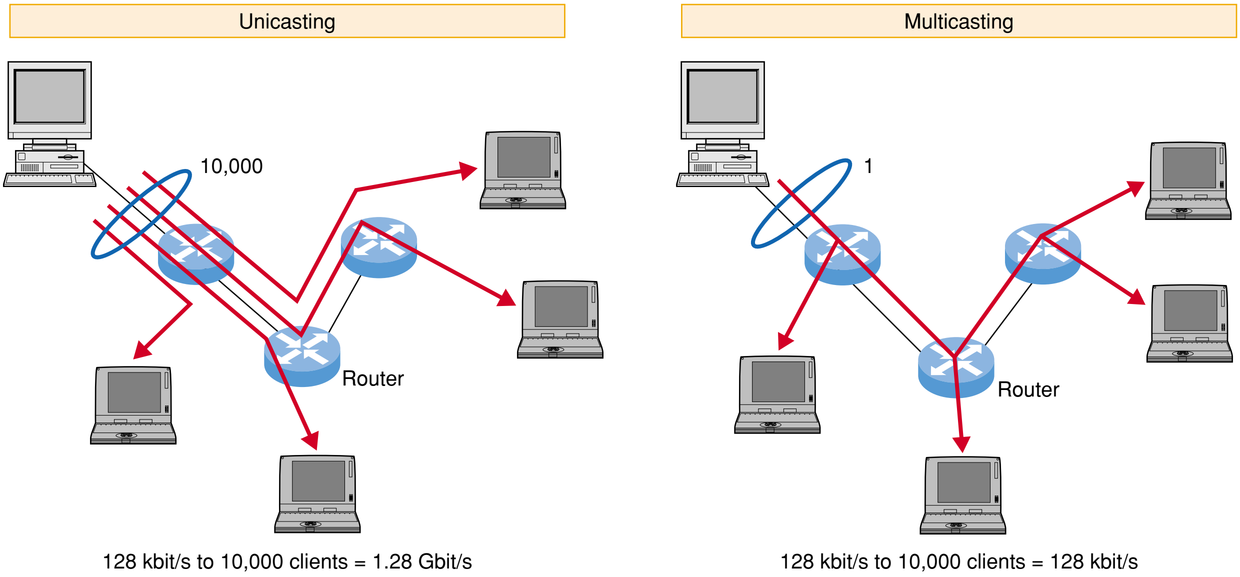
Unicasting
10,000
Router
128 kbit/s to 10,000 clients = 1.28 Gbit/s
Multicasting
1
Router
128 kbit/s to 10,000 clients = 128 kbit/s

Fig. 1. Improvement in network utilization achieved by multicasting (example).

[†] NTT DoCoMo Inc.
Yokosuka-shi, 239-8536 Japan

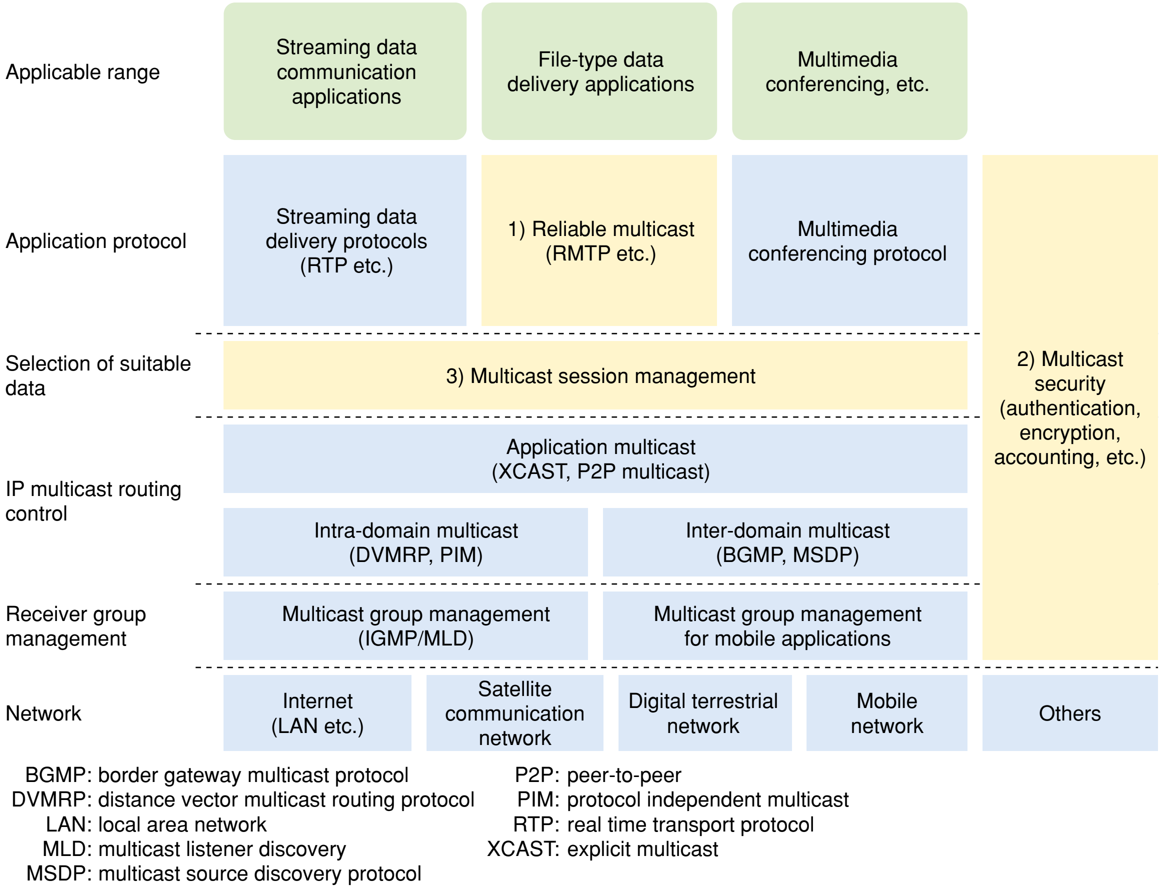
Applicable range
Streaming data communication applications
File-type data delivery applications
Multimedia conferencing, etc.
Application protocol
Streaming data delivery protocols (RTP etc.)
1) Reliable multicast (RMTP etc.)
Multimedia conferencing protocol
2) Multicast security (authentication, encryption, accounting, etc.)
Selection of suitable data
3) Multicast session management
IP multicast routing control
Application multicast (XCAST, P2P multicast)
Intra-domain multicast (DVMRP, PIM)
Inter-domain multicast (BGMP, MSDP)
Receiver group management
Multicast group management (IGMP/MLD)
Multicast group management for mobile applications
Network
Internet (LAN etc.)
Satellite communication network
Digital terrestrial network
Mobile network
Others
BGMP: border gateway multicast protocol
DVMRP: distance vector multicast routing protocol
LAN: local area network
MLD: multicast listener discovery
MSDP: multicast source discovery protocol
P2P: peer-to-peer
PIM: protocol independent multicast
RTP: real time transport protocol
XCAST: explicit multicast

Fig. 2. Technology fields related to multicasting.

the Internet. It has already been the subject of various studies involving applications in various technical fields such as receiver group management, IP multicast routing control, and application protocols (**Fig. 2**). Examples of these applications using IP multicasting include streaming data delivery applications such as TV broadcasts and bulk data delivery applications such as the delivery of electronic newspapers and Java[*1] programs. It has also been applied to small-scale group communications such as multimedia conferencing systems. In recent years, commercial services using IP multicasting have become available, such as video delivery applications on ADSL (asymmetric digital subscriber line). Meanwhile, the 3rd Generation Partnership Project (3GPP) has been working towards international standardization of multimedia broadcast/multicast service (MBMS) schemes to implement diverse data delivery in mobile communication networks [1]. However, services that use multicasting have yet to become widespread, and numerous technical issues and business model shortcomings have been identified.

In this article, we describe the latest technical trends and our own efforts, focusing on three essential technologies from the technical fields shown in Fig. 2.

1) Reliable multicasting

Because IP multicasting uses UDP (user datagram protocol) in the transport layer, it cannot recover lost data. To provide bulk data delivery applications, it is essential to be able to fully recover the original data, so any lost data must somehow be recovered. In IP multicasting, it is not possible to recover data by retransmission as the same way as in unicasting. However, it is possible to use data encoding techniques to generate redundant data that can be used for all the clients requiring data recovery when targeting multiple clients. Also, since wireless networks with larger fluctuations in error rate require retransmission to ensure that there are no data losses, it is effective to provide schemes that combine retransmission with

[*1] Java is an object-oriented development environment for networks promoted by Sun Microsystems, USA.

data encoding techniques that minimize the traffic overhead caused by retransmission.

2) Multicast security

IP multicasting is designed to be scalable so that it can cope with growing numbers of clients. It therefore uses an anonymous model whereby the clients participating in a group are not explicitly specified in the server (the data sender). In this anonymous model, it is impossible to ascertain the number of clients receiving the data (viewing rate) or to bill them for the service, which are requirements for advertising-based business models. That is one of the reasons why IP multicasting has not become popular yet. For the above reasons, it is necessary to implement some form of client authentication. It is also necessary to use encryption techniques to prevent data from being received by clients that do not have access authorization.

3) Multicast session management

In IP multicasting, clients must select their desired group (multicast address) and then perform the subscription procedure for this group in order to start receiving data. On the other hand, schemes in which the server adaptively indicates groups that the client wants to receive are now being researched. In such a server-led scheme, up-to-the-minute data can be provided straight away to the clients, enabling the implementation of responsive realtime and push-type data delivery services such as news bulletins. This also has the advantage of reducing the effort of group selection on users and supports users of low-performance terminals such as mobile terminals with limited input and display functions. These technical fields are discussed in greater detail below.

2. Reliable multicast for the recovery of lost data

Reliable multicast (RM) is a multicast technique that offers the reliability (detection of data loss, notification, retransmission, and guaranteed order) that TCP (transmission control protocol) does for IP. Numerous RM techniques have already been proposed [2], and advances have been made not only in the basic reliability assurance functions but also in the investigation of more advanced functional enhancements such as flow control, congestion control, forward error correction (FEC), and applications to mobile Internet services. Standardization activities in IETF (Internet Engineering Task Force) aimed at spreading RM are also well under way [2].

2.1 Reliable multicast transport protocol

The most important of the RM technologies is the reliable multicast transport protocol (RMTP) [3], which was jointly developed by NTT and IBM Japan. This protocol can deliver data to multiple clients by multicasting without errors while maintaining the same reliability as TCP. The main functions of RMTP are connection management such as the establishment and release of connections between the server and clients, data delivery by IP multicasting, sequence control whereby data is guaranteed to be delivered to the client in the same order as it is transmitted from the server, retransmission control for lost packets using the sequence numbers assigned to the transmitted packets, transmission rate control for the server according to the reception status of the clients, and back-off control to adjust the timing of response transmission from the clients to avoid the responses from clients concentrating at the server.

An example of an RMTP sequence is shown in **Fig. 3**. Data delivery by RMTP consists of a connection-setting phase, a data delivery and retransmission phase, and an individual retransmission phase. In the connection-setting phase, the server informs the clients that it is starting the data transmission. Clients that receive this notification respond to the server with a confirmation of the connection settings. In the data delivery and retransmission phase, the server splits the data into multiple packets and delivers them using IP multicasting. Clients that receive the final packet transmit either an ACK (acknowledgment) or a NACK (negative acknowledgment) to the server according to the reception status. The server releases the connections to the ACK clients, while for NACK clients it retransmits the data corresponding to the packet numbers listed in the NACK messages. This process is repeated until the server receives an ACK from all the clients. If for any reason a client is unable to finish the data delivery by IP multicasting and an ACK message cannot be received within a fixed period of time, the server is also able to drop the client from the IP multicast data delivery. When data delivery is resumed for these disconnected clients, it is possible to perform individual retransmission by unicasting.

2.2 Techniques for error recovery in wireless networks

Compared with fixed-line networks, wireless networks are generally characterized by having higher error rates and larger variations in delay times. Therefore, a key issue when implementing multicast deliv-

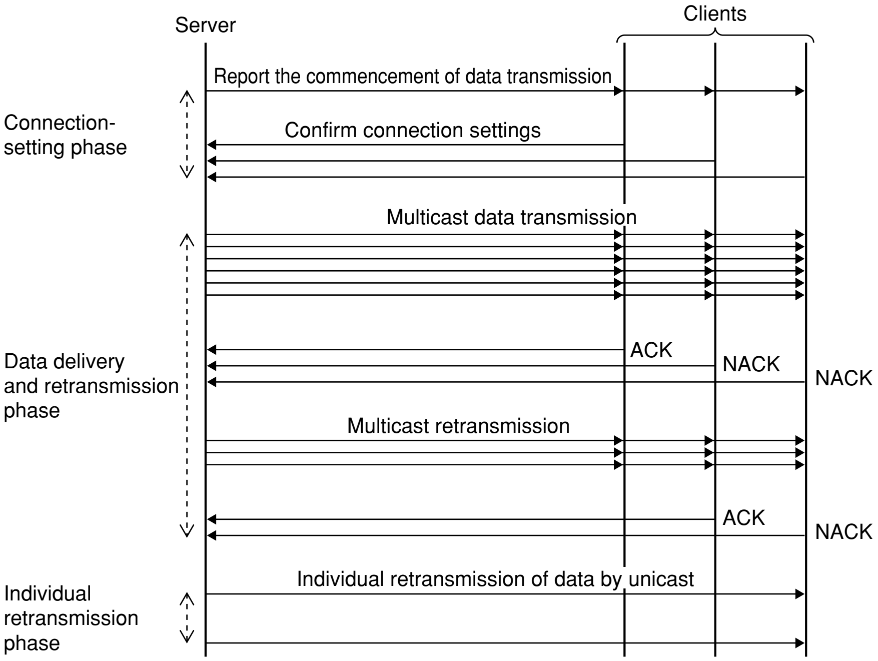
Server
Clients
Report the commencement of data transmission
Connection-setting phase
Confirm connection settings
Multicast data transmission
Data delivery and retransmission phase
ACK
NACK
NACK
Multicast retransmission
ACK
NACK
Individual retransmission of data by unicast
Individual retransmission phase

Fig. 3. Example of an RMTP communication sequence.

ery to mobile terminals is to improve their error resilience. In particular, when delivering bulk data, it is essential to ensure that no data is lost.

Typical error recovery techniques include automatic repeat request (ARQ) in which the parts affected by errors are recovered by retransmission, FEC in which redundant data is added by encoding at the server and errors are corrected at the receiving end, and consecutive transmission in which copies of the data are transmitted repeatedly. These techniques can be used in combination, and in particular ARQ and FEC are known to work well together due to their respective error recovery characteristics. Examples include methods in which data losses up to the recoverable limit are corrected by FEC, while losses that partially exceed the recovery limit are recovered by ARQ. To establish an error recovery scheme suitable for wireless networks, we conducted a theoretical analysis in which we modeled the communication performance of existing error recovery techniques (transmission time and number of packets transmitted) and verified the model's validity in experiments using a wireless local area network (WLAN) and a dozen or so notebook personal computers. From the results of analysis using numerical examples, we were able to construct an actual error recovery algorithm that combines ARQ and FEC [4]. Since the encoding parameters of FEC (code length: n; number of data blocks: k) must be determined to suit the properties of the communication network and the application requirements, it is difficult to uniquely determine the encoding parameters when combining two techniques such as ARQ and FEC that have complementary characteristics. We therefore defined an evaluation function based on the communication cost; it consists of the transmission time and the number of packets needed to complete the transmission. Furthermore, we established a method for deriving the encoding parameters so as to minimize the value of this evaluation function [4]. This method can simplify system design by enabling a simulation-based approach whereas it used to be necessary to perform evaluations and verifications based on field trials and operational data. It can also be used to adjust parameter values needed for mixtures of terminals using different types of wireless network. In general, the value that minimizes the transmission time is independent of the value that minimizes the number of packets. The development of a rational method for determining design policies related to which of these should be given priority and what priority level should be given to them is an outstanding issue. For example, greater priority should be given to minimizing transmission times in applications where realtime performance is important or to minimizing the number of packets transmitted in cases where customers are billed according to usage volume based on the amount of data downloaded, as in file delivery services in mobile communication. A parameter design method that uses our evaluation function can derive values that can minimize the transmission costs in terms of both transmission time and the number of packets transmitted with a good balance.

3. Multicast security for encryption and client authentication

From an early stage, the IETF has recognized the importance of data encryption techniques for multicasting to prevent data being used by unauthorized users. It has therefore prescribed a group key management architecture for performing the encryption and key management needed for multicasting (**Fig. 4**). This group key management architecture involves the use of a traffic encryption key (TEK) and a key encryption key (KEK), which are shared among the group members. By using a client individual key (CIK) to provide these keys to each group member, it is possible to encrypt data delivered by multicasting. Since it is envisaged that the KEK will be updated as group members subscribe and unsubscribe, part of our research is aimed at developing a method for updating the KEK while keeping it synchronized among the group members. The IETF is also expanding the Internet protocol security (IPsec) to prescribe a data encryption protocol that uses a TEK to implement the encryption of multicast-delivered data.

The IETF group management architecture allows accounting (billing and user access logging) to be implemented based on information exchanged during key distribution. However, a problem with this architecture has been its inability to perform accounting accurately in synchronization with members subscribing to and unsubscribing from the group. Furthermore, since any client can request the reception of data in the anonymous model of IP multicasting, this form of multicasting has been susceptible to denial-of-service (DoS) attacks where users subscribe to whatever groups they come across. A multicast DoS attack can be constructed without the need for a multicast delivery route, so this is a serious issue affecting the entire network.

After considering these issues, we proposed the receiver authentication and group key delivery protocol (AKDP) that extends the IETF group key management architecture with various protocols. AKDP can authenticate clients synchronously with the delivery of group keys and the migration of clients subscribing to and unsubscribing from the group, thereby allowing accurate accounting to be implemented. Since the clients are authenticated, only authorized clients can join the group. As a result, it is possible to take measures against multicast DoS attacks. This AKDP protocol is based on the Internet Group Management Protocol (IGMP) for multicasting with the addition of client authentication and group key delivery functions. It operates by linking the clients together with a router incorporating the AKDP (AKDP router) and a key management server that stores the client authentication information and KEK data (**Fig. 5**). When we proposed AKDP, we therefore had to verify the scalability issues caused by an increase in the number of clients and the service performance reduction caused by the longer processing times. Using prototype software, we verified that an AKDP client authentication sequence and group key

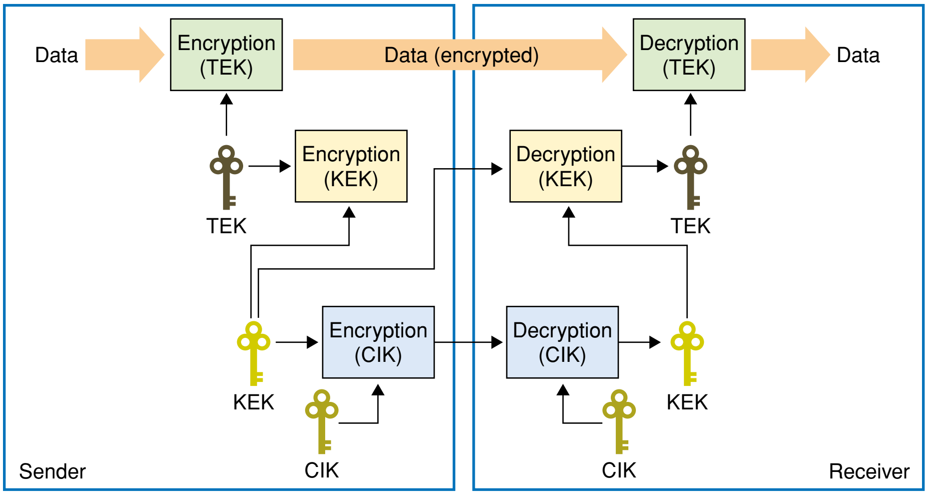

Fig. 4. Group key management architecture.

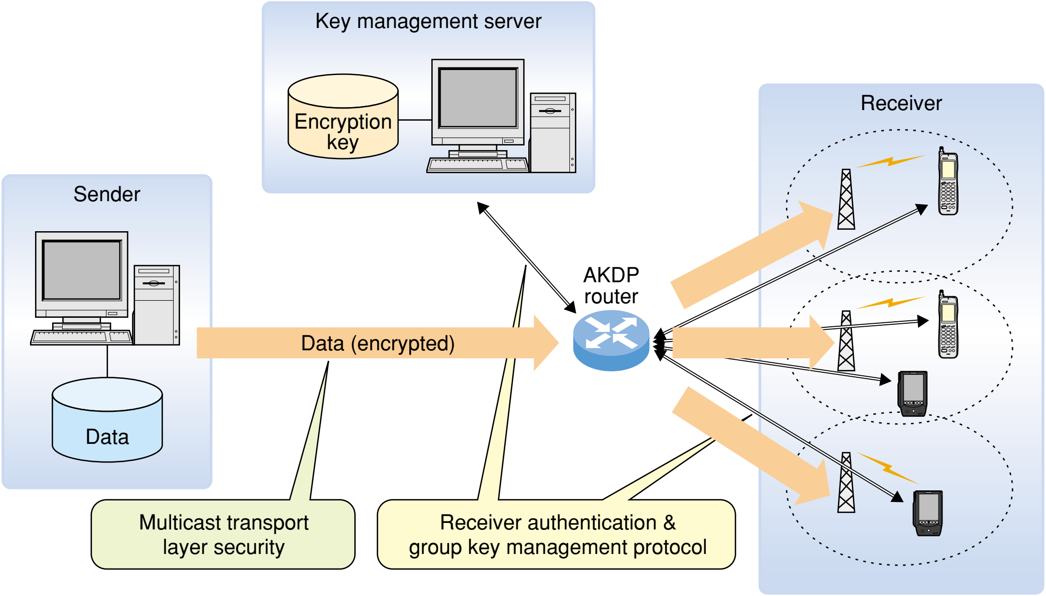
Key management server
Encryption key
Sender
Data
Receiver
AKDP router
Data (encrypted)
Multicast transport layer security
Receiver authentication & group key management protocol

Fig. 5. Multicast security architecture and protocol.

delivery process can be completed in a few hundred milliseconds. We also confirmed that no problems occurred when an AKDP router was simultaneously accessed by a typical number of clients (access from 256 terminals in 1 ms) [5].

We have also proposed a new multicast data encryption protocol for the transport layer called multicast transport layer security (MTLS), which can be used by any application, and we have proved its viability by constructing a prototype system and evaluating its performance [6]. MTLS defines an encryption protocol on UDP, which is the transport layer used in IP multicasting. It prescribes a protocol that can be applied to any UDP application, yet is sufficiently simple to be used in mobile communications. In the performance evaluation of MTLS in a prototype system, we obtained a peak throughput of 3.839 Mbit/s, thereby confirming that MTLS can be used for video delivery services in 3G (third generation) mobile communication networks and IEEE802.11b WLAN applications.

As described above, since IP multicasting cannot use the same security techniques as unicasting, numerous studies are being performed to develop security techniques for IP multicasting. Examples of studies not discussed here include an electronic watermarking technique for multicasting that prevents the redistribution of received data, a server access control technique that prevents malicious users from transmitting data, and a transmission source authentication technique that verifies that data is being transmitted from the correct server. When implementing broadcast-type data delivery services using IP multicasting, it is essential to select and apply the required security techniques from various viewpoints, taking into consideration the requirements and constraints of content providers and the cost of protecting data and the value of the data to be protected.

4. Multicast session management for providing users with the optimal data

In IP multicasting, clients initiate the reception of data by selecting the group (multicast address) they wish to receive and following this group's subscription procedure. Consequently, the client must select the group from which to receive data by acquiring metadata (session data) previously related to the data to be delivered. However, when using a mobile terminal with limited input and display functions, such as a mobile phone or a personal digital assistant (PDA), it can be difficult for the user to select a suitable group from large quantities of session data. In particular, when linking to services that exploit the characteristics of mobile terminals, such as positional information, there are likely to be cases where the environment surrounding the user is in a state of constant flux with every change affecting the data that the user wants to receive. This makes the load on users for selecting suitable groups rather large. Focusing on this issue, we proposed a method in which the group

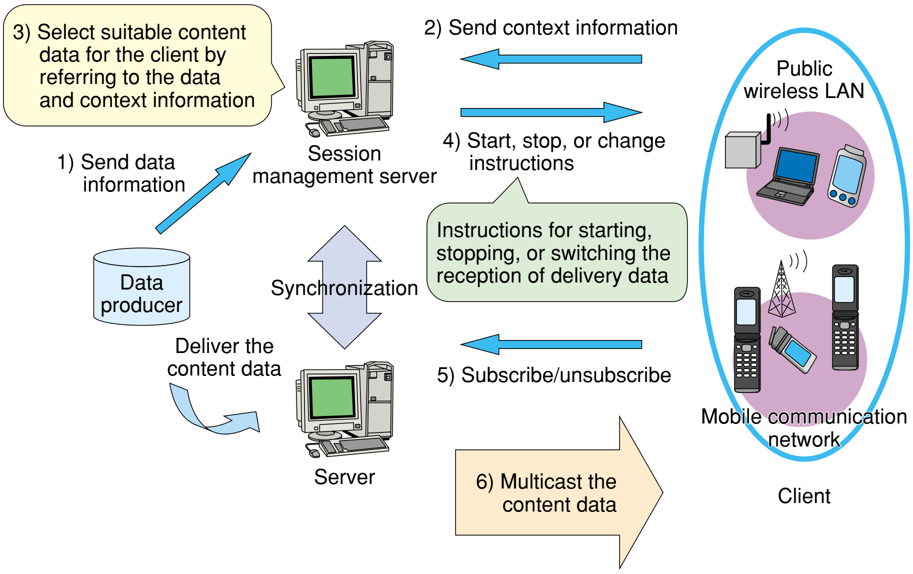
3) Select suitable content data for the client by referring to the data and context information
2) Send context information
Public wireless LAN
1) Send data information
Session management server
4) Start, stop, or change instructions
Instructions for starting, stopping, or switching the reception of delivery data
Data producer
Synchronization
Deliver the content data
5) Subscribe/unsubscribe
Mobile communication network
Server
6) Multicast the content data
Client

Fig. 6. Control flow for multicast session management.

selection processing is performed by a proxy on other equipment [7].

In this proposed scheme, the group selection processing is performed on the network side where the delivery data and session data are maintained. For this purpose, we have defined a new session management server (**Fig. 6**). This server collects two types of information: 1) delivery data information from the data producers such as content providers (including session data such as the title and summary of the data and delivery conditions such as a delivery time) and 2) context information*2 from sources such as the clients and the network equipment (including information about the user such as the user's interests and preferences, and information related to the surroundings such as the temperature and weather conditions). The session management server then selects suitable data to deliver (content data) for the client by referring to the data and context information (step 3) in Fig. 6. After that, the session management server 4) instructs the client to either start receiving from the group that delivers this data, stop receiving this group, or change to a new group. When the client receives this instruction, 5) it automatically starts, stops, or changes the reception of the group according to ordinary IP multicast procedures, thereby making it possible to 6) receive the data delivered at the modified multicast address. Thus, the proposed scheme directly inherits the IP multicast procedures in steps 5) and 6) and provides the new functions in steps 1) through 4).

An example of an application that uses this sort of server-led group switching is a data switching application that operates according to the user's interests and location. In this application, by using the user's context information such as positional information obtained by radio frequency identification (RFID) tags or the global positioning system (GPS) and information about the user's interests that was previously registered by the user, the system enables the user to continue receiving while automatically switching to the content data closest to the user's current location as the user moves.

In this proposed scheme, the ability to freely manage the data delivery conditions and the context information that is used should make it possible to develop applications for new data delivery services. In particular, since it is essential to ensure that the delivery is well targeted in data delivery services that involve the delivery of advertising, there is a need for techniques that appropriately select the data received by the client as in this proposed scheme.

5. Conclusion

Before implementing commercial services, we are resolving technical issues through our recent research and development and international standardization

*2 Context information: Any information that can be used to characterize the status of an entity. An entity is a person, place, or object regarded as having some bearing on the interactions between the user and the application, including the user and application themselves.

efforts related to multicasting. Although there are still many issues that need to be addressed, such as the construction of a business model that allows related businesses to work together to provide broadcast-type data delivery services, and policy issues related to legal matters such as copyright, we think that multicasting will become a key technology for creating new communication media.

References

[1] 3GPP, "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description," 3GPPTS23.246, 2004.

[2] S. Kinoshita, "A survey of reliable multicasting," Trans. IEICE, Vol. J85-B, No. 11, 2002 (in Japanese).

[3] N. Yamanouchi, T. Shiroshita, T. Sano, and O. Takahashi, "A mechanism for reliable multiple address bulk transfer," Trans. IPSJ, Vol. 39, No. 6, 1998 (in Japanese).

[4] H. Suzuki, T. Harashita, K. Tanaka, H. Ueno, and N. Ishikawa, "Comparative evaluations on multicast error recovery methods over wireless LAN," DICOMO2003, Vol. 2003, No. 9, 2003 (in Japanese).

[5] H. Ueno, K. Tanaka, H. Suzuki, N. Ishikawa, and O. Takahashi, "An access control & group key delivery protocol for multicast communication," Second Forum on Information Technology, 2003 (in Japanese).

[6] H. Ueno, K. Tanaka, H. Suzuki, N. Ishikawa, and O. Takahashi, "Proposal and implementation of a transport layer data encryption protocol for multicast communication," Technical Report of IEICE, Vol. l03, No. 122, 2003 (in Japanese).

[7] K. Tanaka, H. Ueno, H. Suzuki, N. Ishikawa, and T. Harashita, "Proposal for Multicast Content Delivery Architecture Using Context Information," DICOMO2003, Vol. 2003, No. 9, 2003 (in Japanese).

Hidetoshi Ueno

Network Management Development Department, NTT DoCoMo Inc.

He received the B.E. and M.E. degrees in engineering from the University of Tsukuba, Ibaragi in 1997 and 1999, respectively. He joined NTT DoCoMo in 1999. He is currently engaged in R&D of mobile Internet technology and in international standardization activities.

Hideharu Suzuki

Manager, Network Management Development Department, NTT DoCoMo Inc.

He received the B.E. and M.E. degrees in engineering from Chiba University, Chiba in 1989 and 1991, respectively. He joined NTT DoCoMo in 1991. He is currently engaged in R&D of mobile Internet technology. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan.

Kiyoko Tanaka

Network Management Development Department, NTT DoCoMo Inc.

She received the B.E. and M.E. degrees in science for open and environmental systems from Keio University, Kanagawa in 2000 and 2002, respectively. She joined NTT DoCoMo in 2002. She is currently engaged in R&D of mobile Internet technology.

Norihiro Ishikawa

Director, Network Management Development Department, NTT DoCoMo Inc.

He received the B.E., M.E., and Ph.D. degrees in information engineering from Kyoto University, Kyoto in 1978, 1980, and 2003, respectively. He joined NTT DoCoMo in 1980. He is currently engaged in R&D of mobile Internet technology and in international standardization activities. He is a member of IEICE and Information Processing Society of Japan.