Special Articles on Multimedia Information Processing

# Multicast Technology for Broadcast-Type Data Delivery Services

*Hidetoshi Ueno, Hideharu Suzuki,*
*Kiyoko Tanaka and Norihiro Ishikawa*

*With the evolution of 3G 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.*
*With this in mind, we have developed protocol techniques relating to 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 to deliver data only to the requested clients, which differs from the broadcasting that simultaneously deliver data to all clients. Compared with unicasting, where data is transmitted to a specific receiver by appointing a single address within the network, multicasting provides an efficient means of transmitting data across networks (**Figure 1**), particularly effective in mobile communication networks where there are limited radio resources available.

Internet Protocol (IP) multicasting is a technique for implementing multicasting on IP networks like 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 (**Figure 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

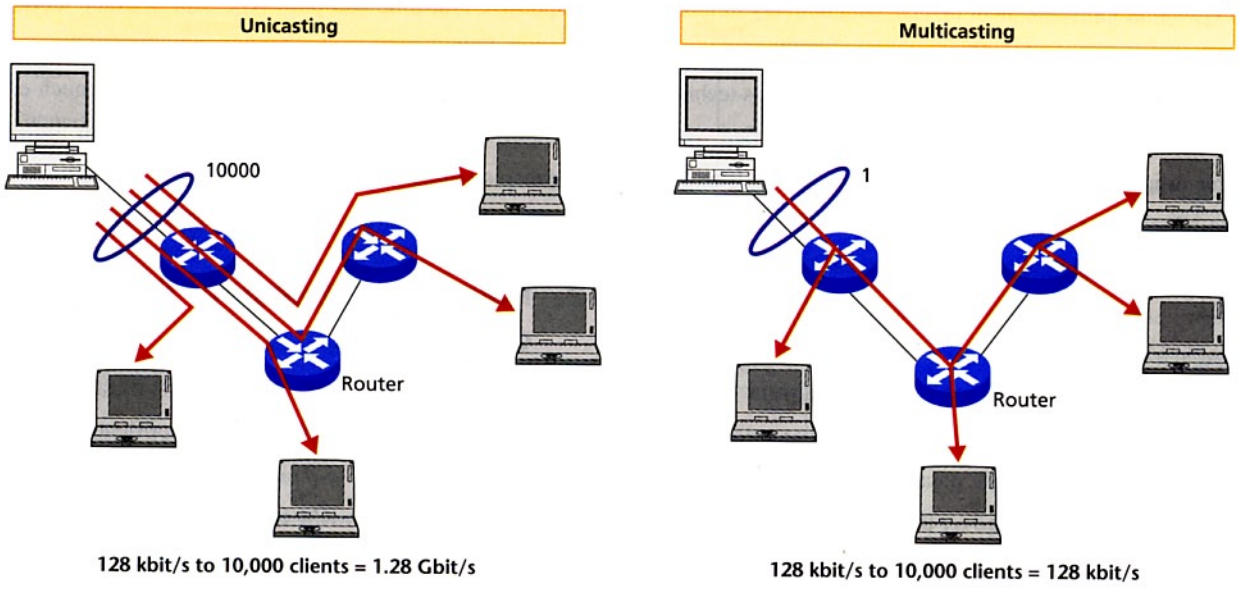
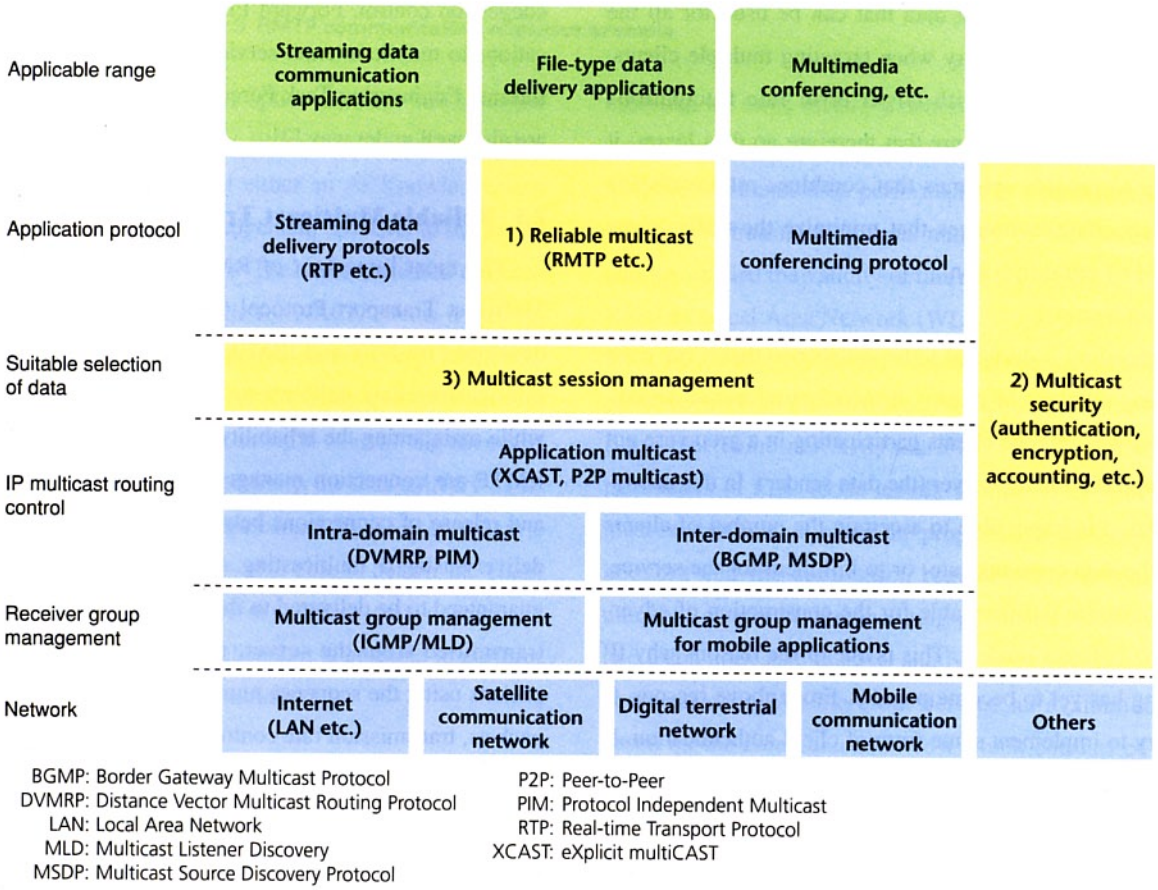



**Figure 1 Improvement of network use efficiency by multicasting (example)**




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

**Figure 2 Multicast technology fields**

delivery of electronic newspapers, 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 Asymmetric Digital Subscriber Line (ADSL). Meanwhile, the 3rd Generation Partnership Project (3GPP) has been working towards the international standardization concerning Multimedia Broadcast Multicast Service

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

(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 shortfalls have been identified.

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

1) Reliable Multicast

Because IP multicasting uses User Datagram Protocol (UDP) in the transport layer, it lacks the ability to recover from data losses. To implement bulk data delivery applications, it is essential to be able to fully recover the original data, so any data losses have to be recovered somehow. In IP multicasting, it is 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, wireless networks with larger error rate fluctuations require retransmission to ensure that there are no data losses, it is effective to provide schemes that combines retransmission with 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 adopts 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 features are indispensable for the construction of advertising-based business models. This is one of the reasons why IP multicasting has yet to become popular. From 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 without access authorities.

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, research is now being conducted into schemes where the server adaptively indicates groups that the client wants to receive. In this server-led scheme, up-to-the-minute data can be provided straight away to the clients, enabling the implementation of responsive real-time and push-type data delivery services such as news bulletins. This also has the advantage of reducing the load on users for selecting groups, and makes it much easier for users of terminals such as mobile terminals with limited input and display functions.

These technical fields are dealt with 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, guaranteed order) as Transmission Control Protocol (TCP) 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 Internet Engineering Task Force (IETF) aimed at spreading RM are also well under way [2].

### 2.1 Reliable Multicast Transport Protocol

The most important of RM technologies is the Reliable Multicast Transport Protocol (RMTP) [3], which was jointly developed by NTT and IBM Japan. This protocol can perform multicasting data delivery to multiple clients without errors while maintaining the 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 using 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 the RMTP sequence is shown in **Figure 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

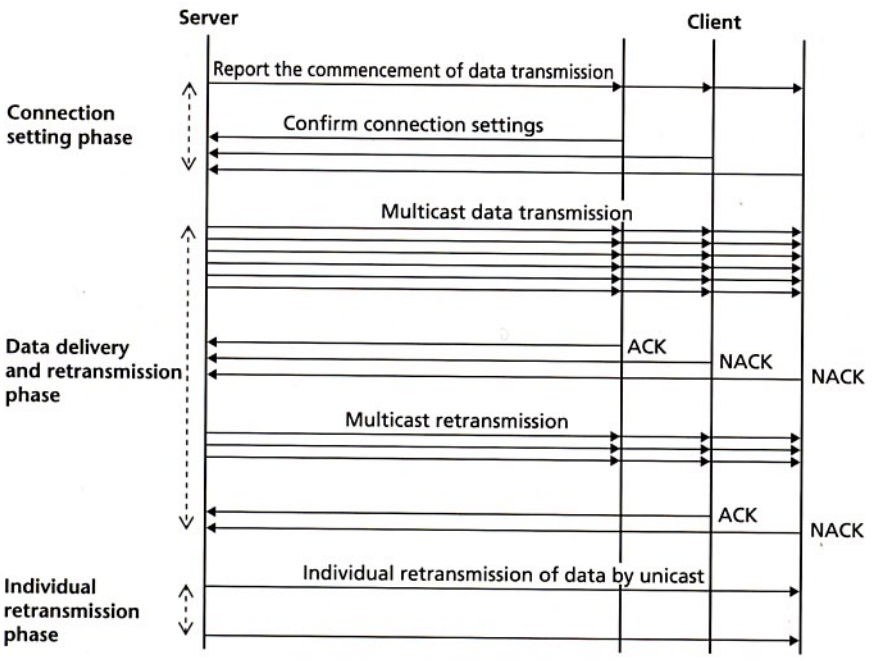



**Figure 3 RMTP communication sequence example**

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 ACKnowledgement (ACK) or a Negative ACKnowledgement (NACK) 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 based on the packet numbers requiring retransmission that were specified 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 cut off 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 a larger variation of delay times. Improving their error resilience is therefore a key issue when implementing multicast delivery to mobile terminals. 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, number of packets transmitted), and we verified the validity of this model in experiments using a Wireless Local Area Network (WLAN) and a dozen or so notebook PCs. 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 which consists of the transmissin time and the number of packets needed to complete the transmission, and we established a method for deriving the encoding parameters so as to minimize value this evaluation function [4]. Using this method, it is possible to simplify the system design by simulations where hitherto it was necessary to perform evaluations and verifications based on field trials and operational data. This technique 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 relating to which and how much of these should be given priority is an issue that remains to be addressed. For example, greater priority should be given to minimizing transmission times in applications where real-time 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 are able to 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 in order to prevent the data reception by unauthorized users. The IETF has therefore prescribed a group key management architecture for performing encryption and the key management needed for multicast (**Figure 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 the multicast delivery data. Since it is envisaged that the KEK will be updated as group members subscribe or unsubscribe, part of our research is aimed at developing a method for updating the KEK while keeping it synchronized between 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 multicast delivery data encryption.

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 that its inability to perform accounting accurately in synchronization with members subscribing or unsubscribing the group. Furthermore, since any client is able to 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, and is thus a serious issue affecting the entire network.

After looking into these issues, we proposed the receiver Authentication and group Key Delivery Protocol (AKDP) that extends the IETF group key management architecture with various protocols. In this proposed protocol it is possible to authenticate clients synchronously with the delivery of group keys and the migration of clients subscribe and unsubscribe from the group, thereby allowing accurate accounting to be implemented. Since the clients are authenticated, only authorized clients are able to join the group, and 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, and operates by linking the clients together with a router incorporating the AKDP (AKDP router) and a key management server that stores the client authentica-

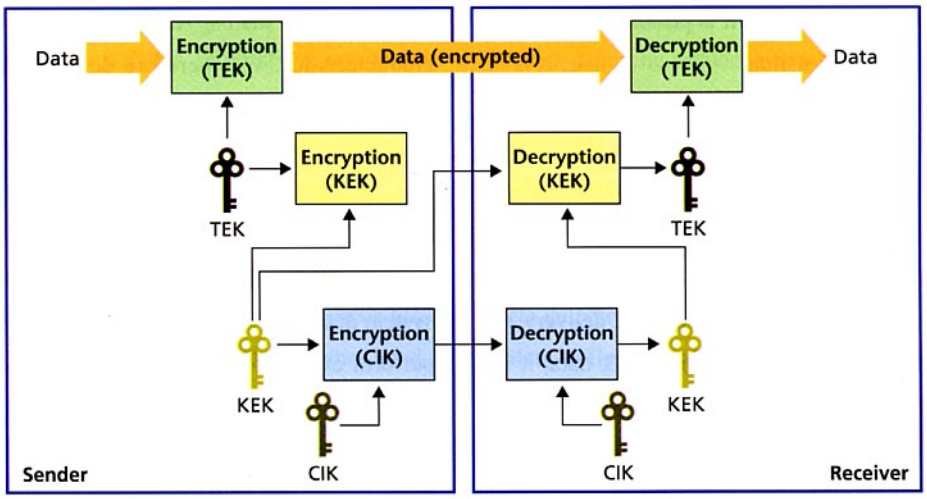



**Figure 4 Group key management architecture**

tion information and KEK data (**Figure 5**). When we proposed AKDP, we therefore had to verify the scalability issues caused by increasing the number of clients and the reduction of service performance caused by the longer processing times. Using prototype software, we verified that an AKDP client authentication sequence and group key delivery process can be completed in a few hundred milliseconds, and we also confirmed that no problems occur when an AKDP router is simultaneously accessed by the sort of client numbers generally expected (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, and is characterized in that 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 adequately cope with being applied to video delivery services provided in Third-Generation (3G) mobile communication networks and IEEE802.11b WLAN applications.

As described above, since IP multicasting is unable to adopt 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 electronical 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 a various viewpoint, taking into consideration the requirements and constraints of content providers and the cost 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 terminal 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

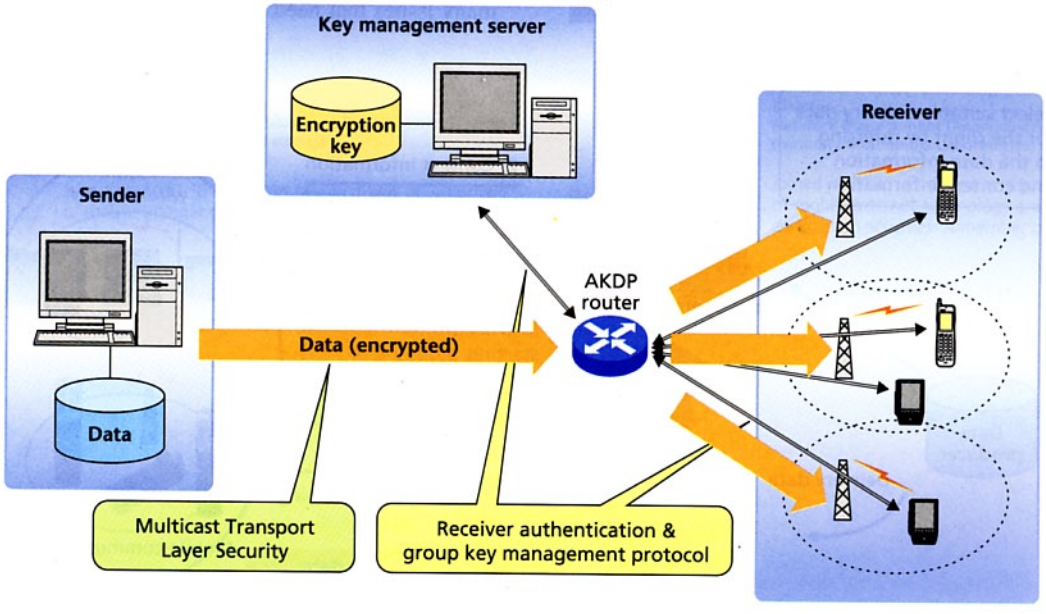



**Figure 5 Multicast security architecture and protocol**

change affecting the data that the user wants to receive, thus resulting in a pronounced load on users for the selection of suitable groups. By focusing on this issue, we have proposed a method in which the group selection processing is performed by 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 (**Figure 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 relating to the surroundings such as the temperature and weather conditions). The session management server then 3) selects suitable delivery data for the client by referring to the data information and context information. After that, the session management server 4) instructs the client to either start receiving from the group that delivers this data (Start), stop the reception of this group (Stop), or change to a new group (Change). 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. In this way, the proposed scheme is characterized in that it directly inherits the IP multicast procedures in steps 5) and 6), and in that it otherwise provides 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 the user's positional information. 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 the user's interests information previously registered by the user, it is possible to continue receiving while automatically switching to the delivery data most closely associated with the user's current location as the user moves.

In this proposed scheme, the ability to freely manage the data delivery conditions and the content of the context information that is used should make it possible to develop applications to new data delivery services. In particular, since it is essential to ensure that the advertising 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

We are in the process of resolving the technical issues towards the implementation of commercial services through our recent research and development and international standardization efforts relating to multicasting. Although there are still many issues that need to be addressed, such as the construction

*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.

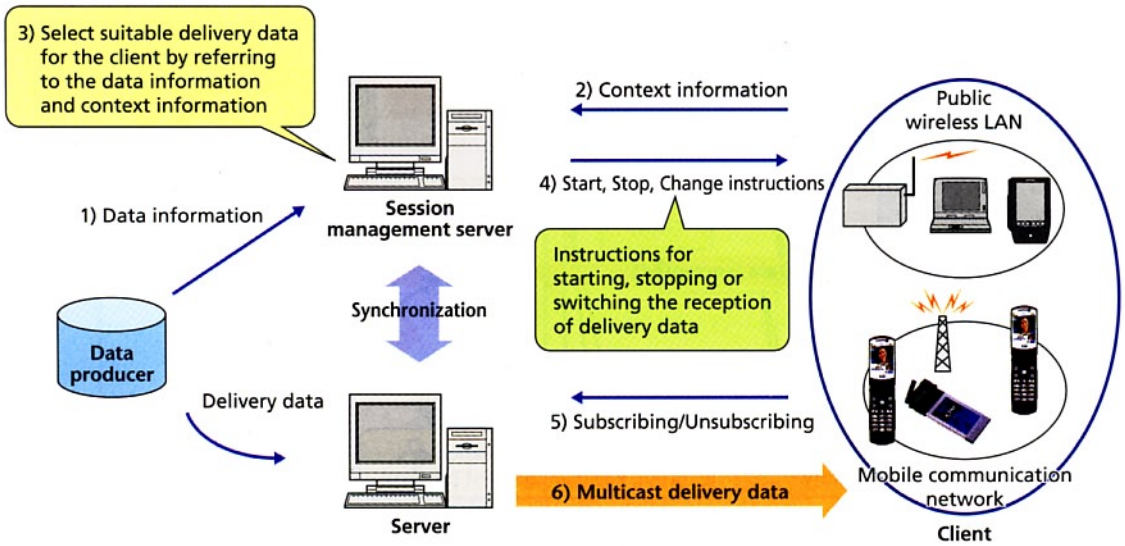



**Figure 6 Control flow for multicast session management**

of a business model that allows related businesses to work together to provide broadcast-type data delivery services, and policy issues relating to legal matters such as copyright, we hope that multicasting will become a key technology for the creation of 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.

[3] N. Yamanouchi, et al.: "A mechanism for reliable multiple address bulk transfer," Trans IPSJ, Vol. 39, No. 6, 1998.

[4] H. Suzuki et al.: "Comparative evaluations on multicast error recovery methods over wireless LAN," DICOMO2003, Vol. 2003, No. 9, 2003.

[5] H. Ueno, et al.: "An access control & group key delivery protocol for multicast communication," Second Forum on Information Technology, 2003.

[6] H. Ueno, et al.: "Proposal and implementation of a transport layer data encryption protocol for multicast communication," Technical Report of IEICE, Vol. I03, No. 122, 2003.

[7] K. Tanaka, et al.: "Proposal for Multicast Content Delivery Architecture Using Context Information," DICOMO2003, Vol. 2003, No. 9, 2003.


## ABBREVIATIONS

3GPP: 3rd Generation Partnership Project
ADSL: Asymmetric Digital Subscriber Line
AKDP: receiver Authentication and group Key Delivery Protocol
ARQ: Automatic Repeat reQuest
BGMP: Border Gateway Multicast Protocol
CIK: Client Individual Key
DoS: Denial of Service
DVMRP: Distance Vector Multicast Routing Protocol
FEC: Forward Error Correction
GPS: Global Positioning System
IETF: Internet Engineering Task Force
IGMP: Internet Group Management Protocol
IP: Internet Protocol
IPsec: Internet Protocol security
KEK: Key Encryption Key
LAN: Local Area Network
MBMS: Multimedia Broadcast Multicast Service
MLD: Multicast Listener Discovery
MSDP: Multicast Source Discovery Protocol
MTLS: Multicast Transport Layer Security
P2P: Peer-to-Peer
PDA: Personal Digital Assistant
PIM: Protocol Independent Multicast
RFID: Radio Frequency IDentification
RM: Reliable Multicast
RMTP: Reliable Multicast Transport Protocol
RTP: Real-time Transport Protocol
TCP: Transmission Control Protocol
TEK: Traffic Encryption Key
UDP: User Datagram Protocol
WLAN: Wireless Local Area Network
XCAST: eXplicit multiCAST