Review

Comparative study of broadcast and multicast in 3GPP and 3GPP2 networks

Jeng-Feng Weng\textsuperscript{a}, Jyh-Cheng Chen\textsuperscript{a,b,*}, Kai-Wen Cheng\textsuperscript{a}

\textsuperscript{a} Department of Computer Science, National Tsing Hua University, Hsinchu, Taiwan
\textsuperscript{b} Institute of Communications Engineering, National Tsing Hua University, Hsinchu, Taiwan

\textbf{Abstract}

Multicast can greatly save network bandwidth because only one copy of data is transmitted in the shared paths. Applications such as video conferences and network games usually can benefit from multicast. Although mobile multicast has been studied for years, it is still a challenge and has not been widely realized in today's Internet. Both 3GPP and 3GPP2 have defined architectures and protocols for multicast. This paper presents the multicast architectures and operations defined in 3GPP and 3GPP2. Besides, this paper also provides a systematic comparison of them. In addition to system architectures, various issues including mobility, QoS, and security are discussed. Moreover, we discuss the challenges in radio resource management (RRM), power control, scalability, and complexity. This paper could be a reference for those seeking the perspective often difficult to obtain from standards specifications.

\textcopyright 2008 Elsevier B.V. All rights reserved.

1. Introduction

Multicast is used for \textit{one-source-many-destination} communications. In multicast, various receivers may share some common paths. Unlike conventional unicast transmission, only one copy of data is transmitted in the shared paths in multicast. Therefore, multicast can greatly save network bandwidth. It could also reduce the sender's load. Applications such as video conferences and network games usually can benefit from multicast. Both IPv4 and IPv6 provide a set of IP addresses for IP multicast. Research on multicast for the Internet has been developed for decades. Many well-known IP multicast protocols have been proposed.

3GPP and 3GPP2 have also defined architectures and protocols for multicast. Although the packet core networks in 3GPP and 3GPP2 can transport IP packets, existing IP multicast protocols cannot apply to them directly. Conventional IP multicast protocols usually do not consider mobility. Although mobile multicast has been studied for years, it is still a challenge and has not been widely realized in the Internet. 3GPP and 3GPP2, however, are designed for mobile and wireless communications. In addition, although the packet core networks of 3GPP and 3GPP2 are based on IP, the architectures are quite different from today's Internet architecture. Besides, standard IP routing is not used. Instead, IP packets are tunneled inside 3GPP and 3GPP2 packet core networks [1]. Therefore, 3GPP and 3GPP2 have defined their own multicast architectures and protocols.

This paper presents an overview of the 3GPP and 3GPP2 broadcast and multicast architectures and protocols. We also provide a systematic comparison of them. We assume readers are familiar with the overall architectures and operations of 3GPP and 3GPP2 systems already. This paper focuses on broadcast and multicast only.

2. Multimedia broadcast/multicast service (MBMS) in 3GPP

In 3GPP, two multicast/broadcast services have been proposed: \textit{cell broadcast service} (CBS) and \textit{multimedia broadcast/multicast service} (MBMS) [2,3]. The CBS is based on \textit{short message service} (SMS) developed in GSM. It provides only text-based service. The MBMS is newly developed for both multicast and broadcast services. It provides not only messaging services but also multimedia services. Furthermore, it is also compatible with Internet multicast services. The following sessions describe the MBMS architecture and its operations, respectively.

2.1. MBMS architecture

Fig. 1 illustrates the MBMS architecture. The architecture is extended from the original 3GPP packet switched (PS) domain. The \textit{broadcast multicast service center} (BM-SC) is a newly introduced component to support MBMS services. The content provider and \textit{multicast broadcast source} are the sources of multicast data. They generally work together as one component although they can also be separated into different entities. The multicast broadcast source only provides multicast data sources. The content provider, however, is also responsible for control information, including subscription, group addresses, and other multicast/broadcast related
information, in addition to providing multicast data sources. Both of content provider and multicast broadcast source can be either within the local domain or outside the 3GPP network. In addition to the three newly introduced components, existing components, such as gateway GPRS support node (GGSN), serving GPRS support node (SGSN), and user equipment (UE), need to support MBMS as well.

The BM-SC is the entry point in 3GPP network for MBMS services. It is located between content provider/multicast broadcast source and GGSN. It supports several functions, including membership, session and transmission, proxy and transport, service announcement, and security functions. Fig. 2 illustrates the relationship between the five functions. The membership function authorizes the UEs that want to activate MBMS services. The session and transmission function schedules the transmission of MBMS sessions. The proxy and transport function acts as a proxy agent for signaling and MBMS data between other functions and GGSN. The service announcement function announces available MBMS services. The security function distributes MBMS security keys for data integrity and confidentiality.

The GGSN receives IP multicast traffic from BM-SC. It then routes the traffic to the corresponding SGSNs by using GPRS tunnelling protocol (GTP). If there is no multicast bearer established already, the GGSN will initiate the process to establish the multicast bearer. It will also tear down the multicast bearers when the bearers are not needed.

The SGSN mainly works on per-user service control, including authentication, authorization, and mobility management. By storing the MBMS UE context\(^1\) of each activated user, SGSN can aggregate the users of the same multicast group into one GTP tunnel. That is, SGSN should de-tunnel the packets from GGSN and forward them to the corresponding UEs. Besides, SGSN should support intra-SGSN and inter-SGSN mobility management. When MBMS data is transmitted to a user, the SGSN should establish \(I_u\) and \(C_u\) bearers. It should also tear down the bearers when they are not used.

UTRAN/GERAN is enhanced for efficient MBMS data transmission. It is responsible for delivering MBMS data from core network to designated UEs. It also needs to deliver MBMS related information, such as MBMS service announcement and paging. Like that in the original 3GPP PS architecture, UTRAN/GERAN is also responsible for intra-RNC and inter-RNC mobility management for MBMS users.

To support MBMS, UE needs to be enhanced as well. It must be able to receive MBMS service announcement and paging information from the core network. It should also be able to activate and deactivate MBMS services. After activating certain MBMS services, an UE then can receive MBMS data.

The temporary mobile group identity (TMGI) is used to identify a specific MBMS bearer. It contains public land mobile network (PLMN) ID and local MBMS bearer service identifier. Therefore, it is globally unique. When UE activates a MBMS service, BM-SC will allocate a TMGI for this service and deliver it to the UE.

Like the packet data protocol (PDP) context in 3GPP PS domain, MBMS UE context is used to store UE-related MBMS bearer information. It is created by UE, SGSN, GGSN, and BM-SC when an UE activates the MBMS service. In UE and SGSN, MBMS UE context is part of the mobility management (MM) context, which is maintained for each UE. In GGSN, however, there is only one MBMS UE context shared by group of UEs which belong to the same MBMS service.

The MBMS bearer context stores information about the MBMS bearer. The information includes quality of service (QoS) parameters, number of UEs, and a list of routing areas that the UEs join. The MBMS bearer context is created and preserved in the nodes which need to transmit MBMS data. MBMS bearer context has two states: standby state and active state. In standby state, no MBMS bearer exists for MBMS data delivery. On the other hand, there is a MBMS bearer to transmit MBMS data in active state. The transition of the two states is triggered by session start or session stop which will be discussed in next section.

2.2. MBMS operations

This section presents the procedures for using MBMS services. Fig. 3 depicts the procedures for multicast mode. The broadcast mode is same except that it does not include steps (1) subscription, (3) joining, and (8) leaving.

In Step (1) subscription, users establish connection to service providers in order to receive MBMS related information. The sub-

---

\(^1\) Details of MBMS UE context will be described later.
scription records will be kept in BM-SC. After that, users can find out what services are provided by Step (2) service announcement/discovery, which enables users to discover the range and capability of the MBMS content providers. Several announcement/discovery mechanisms have been proposed: (a) using CBS to broadcast SMS to carry information, (b) advertising services by other MBMS services which have been activated, (c) using PUSH mechanism, such as wireless access protocol (WAP), to inform the users automatically, and (d) using simple uniform resource locator (URL) to query content providers.

If a mobile station is interested in the service, it will subscribe to the service by using Step (3) joining, which will establish signaling connections between the UE and the core network. The UE will send internet group management protocol (IGMP) join message in the activated PDP context to GGSN. After the UE is successfully authorized by BM-SC, the MBMS UE context is created and stored in BM-SC, GGSN, SGSN, and UE. That is, the signaling path from UE to BM-SC is established.

Although the signaling path has been established, it still needs to establish data bearer. Step (4) session start will establish the necessary data bearer. The process is initiated by BM-SC when BM-SC is ready to send MBMS data. After the session is activated, MBMS session attributes are stored in the necessary SGSNs and GGSNs. The UEs then will be notified of incoming MBMS data by Step (5) MBMS notification. After that, MBMS data is transmitted, which is shown as Step (6) data transfer. Once the GGSN receives MBMS data, it will forward the data to the associated SGSNs by looking up MBMS UE context. The SGSNs will also look up their MBMS UE contexts and notify the RNCs which connect to the UEs of the MBMS group. The RANs then will establish Iu bearers between the RNCs and the UEs. Besides, the RNCs will also establish the radio access bearers (RABs) with the SGSNs. After that, MBMS data can be forwarded to the UEs.

On contrary to Step (4) session start, Step (7) session stop is invoked once the BM-SC has no data to send. After that, the related bearers are released. If the BM-SC wants to send MBMS data again, it should perform Step (4) session start again.

Step (8) leaving is opposite to Step (3) joining. In this process, an UE will send IGMP leave message to the serving GGSN if the UE initiates the leaving process. This process, however, can be also initiated by SGSN, GGSN, or BM-SC. For example, if an UE performs GPRS detach before explicitly deactivating the MBMS services, network nodes, such as GGSN, will initiate the leaving process. After that, the MBMS UE context in all nodes will be deleted. That is, there will be no signaling and data bearers for the UE.

Because mobility management in the original 3GPP PS domain is well defined, the mobility management in MBMS is combined with the one developed in 3GPP PS domain. For example, when performing routing area update (RAU), SGSN will update PDP context and MBMS UE context simultaneously. Besides, the new SGSN will register the MBMS service to its GGSN. The old SGSN will also deregister with the GGSN. With some additional procedures, the MBMS mobility management is accomplished along with the original mobility operations.

Unlike mobility management, the security mechanisms developed in the original 3GPP PS domain cannot meet the requirements of the MBMS services. Ciphering keys in MBMS, for example, must be delivered to a group of UEs, which is different with the unicast key distribution in the original 3GPP PS domain. Therefore, 3GPP has developed specific security techniques for MBMS, including authentication, key distribution, and MBMS data protection [4]. Fig. 4 depicts the MBMS security architecture [4]. There are four

Fig. 2. 3GPP BM-SC architecture.
new keys proposed for MBMS, MBMS request key (MRK), MBMS service key (MSK), MBMS traffic key (MTK), and MBMS user key (MUK). MRK and MUK are derived from general bootstrapping architecture (GBA) key. How to produce GBA key can be found in [5]. MRK is used by BM-SC to authenticate UEs. MUK is used to protect the distribution of MSK. The main purpose of MSK is to protect a certain MBMS session. It is also used to protect the distribution of MTK. MSK is delivered by using multimedia internet keying (MIKEY) [6]. It, however, is not used to encrypt MBMS traffic. The encryption and decryption is done by using MTK. In MBMS, some UEs may leave the broadcast/multicast group after certain time. To avoid deregistered UEs from eavesdropping the ongoing MBMS data, BM-SC must update the MSK. The detailed update procedure can be found in [4]. Basically, the MUK will be invalid for the deregistered UEs. Therefore, the deregistered UEs cannot get the correct MSK and MTK. Thus, they cannot receive the ongoing MBMS data.

For QoS, MBMS service only supports background and streaming classes [3]. Background class is used for messaging or file downloading services. Transmission delay is not stringent. Streaming class is used for streaming services, such as video streaming. It must guarantee transmission delay. However, it is almost impossible for all RANs of the same MBMS group to guarantee the required QoS simultaneously. To keep the same QoS level, some RANs may need to transmit MBMS traffic even though the channel condition is bad. As a result, both classes may cause higher service data unit (SDU) error ratio. To lower the SDU error ratio, two possible methods can be used [3]. One is to transmit redundant packets. The other way is to retransmit lost MBMS data. Besides, there is also no QoS negotiation for MBMS bearers. UE cannot negotiate for a specific QoS level because all MBMS data delivered in the same multicast tree must have the same QoS level. A newly joined UE should not request for a higher QoS level. Otherwise it will be rejected. In MBMS, packets in background and streaming classes are categorized into different priorities. In order to ensure the QoS of high-priority MBMS bearers, packets with lower priorities will be dropped.

3. Broadcast-multicast service (BCMCS) in 3GPP2

The broadcast-multicast service (BCMCS) in 3GPP2 networks is designed to provide efficient mechanism to transmit the same information from a single source to multiple users [7–9]. One of the major motivations of BCMCS is to optimize the utilization of cdma2000 radio networks when transmitting the same information to multiple users. The information transmitted in BCMCS is
called BCMCS content stream, which could be any type of data, including text, video, audio, voice, and streaming media.

The BCMCS is classified into two modes: dynamic broadcast mode and static broadcast mode. In dynamic broadcast, bearers are established based on the presence of users. That is, there is no BCMCS bearer unless some users trigger it. This mode is usually used for multicast service. In static broadcast, the operator provides static bearers regardless of the user presence. That is, the bearer will not be changed because of user movement. This mode is normally used for broadcast service.

### 3.1. BCMCS architecture

Fig. 5 depicts the high level view of the BCMCS architecture. Fig. 5 shows that there are six newly introduced components, which are shown in gray level. Note that the figure shows three BCMCS content provider (BCMCS-CP) which can be located in serving network, home network, or any other IP networks. broadcast serving node (BSN), BCMCS controller, BCMCS content server (BCMCS-CS), and multicast router (MR) are located in the serving network. In the architecture, multicast router (MR) is optional. BCMCS subscriber profile manager is located in the home network.

The BCMCS content, which will be delivered to the BCMCS-CS, is originated from any of the BCMCS-CP. The BCMCS-CS is regarded as the content source in the serving network. It may need to merge and reformat the BCMCS content received from different BCMCS-CPs. The BCMCS-CS then forwards the BCMCS content to base station controller (BSC)/packet control function (PCF) through BSN.

MR is located between BSN and BCMCS-CS. It functions similarly to the multicast router defined in the IETF multicast protocols. However, traffic from BCMCS-CS to BSN may or may not go through MR.

In 3GPP2, unicast traffic is processed by packet data serving node (PDSN). BCMCS traffic is processed by BSN, which communicates with BCMCS-CS by using IP multicast protocol to support IP multicast flows. Besides, BSN also communicates with BSC/PCF to add and remove IP multicast flows.

The major role of BSC/PCF in BCMCS is to signal, establish, and separate bearers between mobile station (MS) and BSN. Besides, BSC will choose the best bearer for a MS. PCF will choose the best BSN if QoS is provision for optimal resources.

BCMCS controller manages the BCMCS session information and provides the BCMCS session information to the following entities: (1) radio access network, through the authentication, authorization, accounting (AAA) server in the serving network (referred to as S-AAA), (2) BSN, also through S-AAA, (3) MS, through PDSN, and (4) BCMCS-CS. In BCMCS security framework, BCMCS Controller will also authenticate BCMCS users and BCMCS content providers. Besides, BCMCS controller will generate and distribute security keys for BCMCS. In addition, BCMCS controller may also coordinate the delivery of BCMCS content to the BCMCS-CS.

When users wish to use multicast service, they need to subscribe to specific services. The subscriber profile database in home network stores the BCMCS subscription profiles. The BCMCS subscriber profile manager is responsible for updating and managing the subscription profiles. The AAA server in home network (referred to as H-AAA) may access the subscriber profile database to acquire necessary data to perform AAA functions.

### 3.2. BCMCS operations

The basic procedures for an MS to receive BCMCS service can be divided into seven steps, which are illustrated in Fig. 6.

1. **Service discovery/announcement:** The major role of service discovery/announcement is to distribute the BCMCS information to MSs. An MS can either wait for the announcement from the core network, or discover the service information by itself. If an MS wishes to discover the BCMCS information actively, it will contact with a BCMCS controller. The MS can find the location of a BCMCS controller through H-AAA.
controller either by static BCMCS controller discovery or dynamic BCMCS controller discovery [9]. In the static one, the IP address of the BCMCS controller is preconfigured. In dynamic discovery, specific dynamic host configuration protocol (DHCP) options are used to discover a BCMCS controller [10]. After that, the MS is regarded as a client to communicate with the BCMCS controller, which acts as a server. The server–client communication can be done by using SMS or WAP. Therefore, the MS can get the information about BCMCS content and schedule.

(2) Content subscription: Before receiving BCMCS content, an MS needs to subscribe to the service with the BCMCS subscriber profile manager. The subscription is done by out of band mechanisms. For instance, it may be done by using the web site of the service provider. Besides, a registration key (RK) is used in both user identification module (UM) and subscription profile database to encrypt service subscription.

(3) BCMCS information acquisition: The main purpose of the BCMCS information acquisition is to let MSs know the session information of the desired BCMCS service. This procedure is done by using hypertext transfer protocol (HTTP). The session information includes flow identity information, BCMCS application information, BCMCS link layer information, and BCMCS security parameters. The flow identity information contains registration lifetime and the mapping between real multicast IP address and flow identity. BCMCS application information contains the information of the BCMCS service, such as video coding scheme. BCMCS link layer information contains encryption type and algorithms and parameters of header compression. BCMCS security parameters contain the parameters used for the security scheme.

(4) Content availability determination: Once the BCMCS information acquisition is done, an MS can check whether a specific IP multicast flow is available for the MS. After the base station (BS) broadcasts the BCMCS radio configuration information, the MS can obtain the corresponding radio configuration. If the MS cannot obtain the BCMCS radio configuration information from the cdma2000 overhead message, the MS could acquire the desired IP multicast flow through the BCMCS registration procedure. If the desired IP multicast flow for the MS is not available, the core network will inform the MS.

(5)–(7) BCMCS registration, content delivery, and deregistration: After performing BCMCS registration, the subscriber can request to deliver one or more IP multicast flows to the MS. Therefore, the MS can receive the desired BCMCS contents. In static broadcast, the BCMCS bearer path is established or released through static provision at any time. In dynamic broadcast, the setup of the BCMCS bearer path is triggered by the first MS requesting for the service. Once the bearer path is established, the BCMCS content can be delivered to the MS. All bearer paths are released after the MS deregisters for the BCMCS service.

Similar to that in 3GPP, the mobility management in 3GPP2 packet core network is well defined. In 3GPP2 unicast mode, PDSN performs the function of mobile IP foreign agent. However, BSN might communicate with BCMCS content server or MR by standard multicast protocols defined in IETF. Packets are then tunneled inside the core network via multicast bearer formed by using generic routing encapsulation (GRE) (IETF RFC 1701). When moving from one BS to another BS, MS will update its location by the original 3GPP2 mobility operations with related BCMCS flow information. Therefore, the mobility management in BCMCS could be done along with the original 3GPP2 mobility operations.

The major focus of BCMCS security is in dynamic broadcast mode, i.e. in multicast, because only authorized users can join the multicast group to receive BCMCS content streams. There are four new keys proposed for BCMCS: registration key (RK), temporary key (TK), broadcast access key (BAK), and short-term Key (SK). Each RK is unique and for a specific MS. It is stored in both MS and H-AAA. The main purpose of RK is for H-AAA to authenticate MS. The authentication is performed by using challenge-response [1]. That is, the serving network will send a challenge to MS. Both MS and H-AAA will derive the same result based on the RK and the challenge. The respond derived from MS will be sent to H-AAA, which verifies the respond to see whether the MS is legitimate. Because of the importance of RK, it should never leave MS and H-AAA. Instead, a TK which is generated by H-AAA by using the RK and a random number will be transmitted to the BCMCS controller. It is then used to encrypt BAK, which is generated by BCMCS controller and is used as the security key to access certain BCMCS flows. Therefore, each BCMCS flow requires a different BAK. When a MS performs BCMCS information acquisition, the BCMCS Controller will encrypt BAK by using TK and distribute the BAK to the MS. In addition, the BCMCS controller also needs to send BAK to the BCMCS content server and the BSC. Both BCMCS controller and BSC will further generate SK by using the BAK and a random number. The SK is then used to encrypt BCMCS contents. MSs can decrypt the contents by using the same SK which is derived from the same random number and the BAK. An unauthorized user cannot decrypt the contents because it cannot derive the same SK, which originated from the pre-provisioned RK.

Fig. 7 depicts the security functional architecture of BCMCS [11]. When a service provider wishes to send a BCMCS content to a member (an MS) of a multicast group, Steps (1) and (2) specified in Fig. 7 need to be performed before the BCMCS content is encrypted. The subscription manager (SM) may be the H-AAA of the BCMCS. In Step (1), RK is provided to UIM and SM as a shared key. The RK is used to calculate the TK to protect the BAK. In Step (2), the BAK generator (BAKG) generates BAK, determines an identifier BAK_ID and an expire time BAK_Expire. It then distributes the BAK with BAK_ID and BAK_Expire to BAK distributor (BAKD) and SK manager (SMK).

If no member leaves the multicast group, the BAK will not be changed. In such case, Steps (3)–(7) will be performed under a normal procedure to encrypt BCMCS content with the BAK. The SMK generates SK based on BAK and SK random number (SK_RAND). It also updates and distributes the SK to content encryptor (CE),
which encrypts the BCMCS content from content source (CS). The encrypted BCMCS content is then sent to the MS through the serving system. In Step (3), the SKM generates SK based on the BAK and SK_RAND, then distributes SK, SK_RAND, BAK_ID and BAK_Expire to CE. In Step (4), the CS sends BCMCS content to the CE. In Step (5), the CE uses the SK provided by the SKM to encrypt the BCMCS content and sends the BCMCS content with SK_RAND and BAK_ID to the MS. In Step (6), when the mobile equipment (ME) receives the encrypted BCMCS content, it will check whether BAK_ID and SK_RAND have been changed. If BAK_ID and SK_RAND are not changed from the last BCMCS content, the ME will decrypt the received BCMCS content using the current SK and returns the result to the user application programs on the ME. Otherwise, if BAK_ID or SK_RAND have been changed, the ME will request a new SK from the UIM. In Step (7), the UIM calculates the SK based on the BAK and SK_RAND and passes the new SK to the ME. The ME then will use the new SK to decrypt the received BCMCS content.

When any member leaves the multicast group, the BAK will be changed to prevent the left member from using the old BAK to decrypt the BCMCS content. Steps (8)–(11) will be performed with changed or unavailable BAK. In Step (8), the ME sends a BAK request with authentication information based on RK to BAKD. When the BAKD sends the new BAK to UIM through ME, the new BAK needs to be encrypted to prevent the authorized users to grab the new BAK. In Step (9), therefore, the BAKD request a TK from the SM to protect the new BAK. In Step (10), the SM generates TK based on a random number TK_RAND and RK. The SM sends TK and TK_RAND to the BAKD. The SM then discards the TK and TK_RAND. In Step (11), the BKAD uses TK to encrypt the BAK, and sends the encrypted BAK associated with TK_RAND, BAK_ID, and BAK_Expire to the UIM through the ME. The UIM will generate TK from TK_RAND and RK, then use TK to decrypt the encrypted BAK. Details of BCMCS security can be found in [11].

BCMCS should support QoS guarantee for voice, real-time audio, video, and multimedia services. However, QoS negotiation is only allowed between content server and BCMCS controller. Content server will request the resource for BCMCS flow between the content server and BSN. The BCMCS controller then will decide the available resource. After that, the BCMCS controller will inform BSN the QoS parameters. The QoS guarantee in radio access network, however, is not specified yet in the standards.

4. Comparison

This section provides a systematic comparison of 3GPP MBMS and 3GPP2 BCMCS. Sections 4.1 and 4.2 compare the architectures and operations, respectively. Table 1 summarizes the comparison.

4.1. Architectures

Both 3GPP and 3GPP2 introduce new components to support broadcast and multicast. Both systems have content originating component, which is referred to as content provider in general. The content originating component can be located in home network, serving network, or a third party. Content scheduling and session management are provided by different components. BCMCS content server is responsible for content scheduling, and BCMCS controller deals with session management.

Both MBMS and BCMCS provide content routing. In 3GPP, the routing function is included in BM-SC. When BM-SC receives data from content provider, it will route the data to GGSN. In 3GPP2, BCMCS content server is responsible for routing. In addition, 3GPP2 also supplies MR, located between BCMCS content server and BSN, to help content routing. Both 3GPP and 3GPP2 upgrade...
Architecture  

<table>
<thead>
<tr>
<th>Operation</th>
<th>3GPP</th>
<th>3GPP2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content origination</td>
<td>Content provider</td>
<td>BCMCS Content provider</td>
</tr>
<tr>
<td>Content scheduling</td>
<td>BM-SC</td>
<td>BCMCS content server</td>
</tr>
<tr>
<td>Session management</td>
<td>BM-SC</td>
<td>BCMCS controller</td>
</tr>
<tr>
<td>Content routing</td>
<td>BM-SC</td>
<td>BCMCS content server and MR</td>
</tr>
<tr>
<td>Place to store</td>
<td>HLR</td>
<td>Subscriber profile database</td>
</tr>
<tr>
<td>subscription profile</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low bit-rate message-based service</td>
<td>CBS</td>
<td>None</td>
</tr>
<tr>
<td>Per-user service control</td>
<td>GGSN</td>
<td>BSC/PCF</td>
</tr>
<tr>
<td>Managing unicast IP flows</td>
<td>GGSN</td>
<td>PDSN</td>
</tr>
<tr>
<td>Managing multicast IP flows</td>
<td>GGSN</td>
<td>BSN</td>
</tr>
</tbody>
</table>

5. Challenges

In this section, we discuss challenges in MBMS and BCMCS. The discussions include radio resource management (RRM), power control, scalability, and complexity.

5.1. Radio resource management (RRM)

With the rapid growth of real-time multimedia services and the high number of mobile users, the role of RRM is more important. The basic tasks of RRM include admission control, channel assignment, power control, and handoff. Because radio resource is limited, how to use RRM to provide efficient utilization of the radio resource and guarantee QoS for more mobile users are big challenges in MBMS and BCMCS.

5.1.1. RRM in MBMS

The details of RRM in 3GPP can be found in [12–15]. The basic channels in 3GPP are classified into logical channels, transport channels, and physical channels. There are two transmission models in MBMS channel structure. One is point-to-point (p-t-p). The other one is point-to-multipoint (p-t-m). In p-t-p transmission model, the MBMS control information and user data information are transferred through dedicated control channel (DCCH) and dedicated...
traffic channel (DTCH), respectively. More details of the p-t-p transmission can be found in [16].

The implementation of MBMS in 3GPP requires four new channels: three logical channels and one physical channel as follows:

1. MBMS point-to-multipoint control channel (MCCH) is a logical channel. In radio resource control (RRC) connected mode or idle mode, MCCH is used to transmit control-plane information between network and UEs in the p-t-m downlink transmission.

2. MBMS point-to-multipoint traffic channel (MTCH), which is a logical channel to transmit user-plane information between network and UEs in RRC connected mode or idle mode for a p-t-m downlink transmission.

3. MBMS point-to-multipoint scheduling channel (MSCH) is also a logical channel. In RRC connected or idle mode, MSC is used to transmit MBMS service scheduling between network and UEs for a p-t-m downlink transmission.

4. MBMS notification indicator channel (MICH) is a physical channel used by the network to inform UEs regarding the available MBMS information on MCCH.

Besides, forward access channel (FACH) and secondary common control physical channel (S-CCPCH) are used as the transport channel and physical channel to carry MCCH, MTCH, and MSC.

In p-t-p transmission mode, the high speed downlink packet access (HSDPA) [17–19] can be used to transmit MBMS services by using the high speed physical downlink shared channel (HSDSCH). Because HSDPA employs fast link adaptation, it can provide better performance in links [15]. In p-t-m transmission mode, MBMS services are transmitted over the S-CCPCH. Because S-CCPCH lacks of link adaptation and power control, the link performance of p-t-m is less than that of p-t-p. In [20], authors propose p-t-m over HSDPA. With dynamic system level simulations, the results show that the proposed technique can get better performance ranging from 25% to 70% than the p-t-m without link adaptation. To provide optimal distribution of QoS in MBMS service, Soares et al. [21] analyze several effective radio resource management schemes such as non-uniform QAM, multi-code, and macro-diversity depending on the location of mobile stations. The multi-code and non-uniform 16-QAM can reduce the channel power of p-t-m mode in MBMS. To effectively increase the throughput and the number of multicast services, the non-uniform 16-QAM receiver needs to be built in MBMS with or without the macro diversity combining.

5.1.2. RRM in BCMCS

The radio resource management of cdma2000 can be found in [14]. There are two types of cdma2000 physical channels: dedicated physical channel (DPCH) and common physical channel (CPCH). The BCMCS channel structure consists of two channels: forward supplemental channel (F-SCH) and forward fundamental channel (F-FCH). F-SCH and F-FCH are in DPCH. For an MS, there are two states in BCMCS: idle state and traffic state. We can classify BCMCS into three types based on different radio channels [22–24]:

1. In type 1 BCMCS, the F-SCH is shared between idle MSs. Due to the limited capacity of the reserve link, the type 1 BCMCS does not require reserve link. In this type, the handoff procedure does not require any additional handoff signaling. The BCMCS parameters and configuration information are periodically sent to MSs along with the BCMCS-specific upper layer message. The Reed-Solomon outer encoding is optional to improve the power efficiency. It can also enhance the transmission reliability of the shared F-SCH among MSs.

2. In type 2 BCMCS, the F-FCH is shared among active MSs. In traffic state, the F-FCH is used to transmit common BCMCS content, such as real-time video, to multiple MSs. Time division multiplexing (TDM) is used in this type. The power control is carried by the forward common power control channel (F-CPCCH). The individual signaling of each MS is transmitted on the forward dedicated control channel (F-DCH). The type 2 BCMCS can support soft handoff. It also supports dynamic coverage and can optimize the power consumption of base stations.

3. In type 3 BCMCS, the F-SCH is shared between active MSs. In traffic state, the shared F-SCH is assigned to all BCMCS MSs.

5.2. Power control

With more and more multimedia applications, power control in mobile stations becomes a significant issue in MBMS and BCMCS. Two different approaches can be used to reduce the power consumption. The first approach does not modify the existing MBMS model [25]. The authors propose a power control technique by selecting the most effect transport channel between dedicated and common channels. This technique can reduce the transmission power of the node B in every BS with multicast users in the MBMS network. The second approach extends the existing MBMS model [26]. The authors design multiple content variant (MCV) MBMS to distribute multiple variants of the same content to heterogeneous receivers. This approach can maximize the number of potential users and does not consume extra transmission power.

5.3. Scalability

The scalability of traditional IP multicast mostly focuses on the dynamic join and leave in a large multicast group. The previous studies solve this problem by various scalable multicast key management [27–30]. In MBMS and BCMCS, operators need to add some new components such as BM-SC in MBMS, and BSN, BCMCS-CS, MR, BCMCS-CP, BCMCS Controller, BCMCS subscriber profile manager in BCMCS. To serve more users, operators can deploy these equipments and add new BSs. In MBMS, the problem of multicast key management is solved by MIKEY. BCMCS uses BAK management to achieve dynamic join and leave in large scalable multicast group. One of the important issues of scalability in MBMS and BCMCS is in mobile stations. With the rapid increase of real-time multimedia services in MBMS and BCMCS, mobile stations need to support numerous MBMS/BCMCS applications. This will increase the complexity of a mobile station not only in hardware but also in software and user interface.

5.4. Complexity

Alexiou et al. propose a way to evaluate the cost of the MBMS multicast mode [31,32]. The authors analyze the performance in terms of packet delivery cost under different cell configurations, different user distributions, and different transport channels. There are two types of routing areas (RAs) in the simulation environment. The type 1 RA has multicast user population of 1/2 and the type 2 RA has multicast user population of 1. If $\delta < 1$, most of multicast users belong to type 1 RA. They assume the proportion of type 1 RA is $\alpha$, and the proportion of type 2 RA is $1 - \alpha$. The simulation results show that the cost of the broadcast mode is constant. In addition, when $\delta$ increases, the number of type 2 multicast users increases rapidly. It will result in the decrease in $\alpha$, which means that the total cost increases. The result shows that the complexity of packet delivery in MBMS is affected by the multicast model with
large number of users. This approach could also be used to evaluate the performance of BCMCS in cdma2000.

6. Summary

In this paper, we present the multicast architectures and operations defined in 3GPP and 3GPP2. In addition, we also provide a systematic comparison of 3GPP MBMS and 3GPP2 BCMCS. Various issues including mobility, QoS, and security have been examined in this paper. Many of them are based on the packet-switched core networks which have been developed in 3GPP and 3GPP2. Security, however, needs to be redesigned. Ciphering keys, for example, must be delivered to a group of users. To avoid deregistered users from eavesdropping the ongoing multicast session, the ciphering keys must be updated once a user leaves the multicast group. Both 3GPP and 3GPP2 have proposed new security keys and mechanisms to achieve the objective. They have been discussed and compared in this paper. We also discuss the challenges, include radio resource management (RRM), power control, scalability, and complexity, in MBMS and BCMCS. This paper could be a reference for those seeking the perspective often difficult to obtain from standards specifications.

Acknowledgement

This work was sponsored in part by National Science Council (NSC) under the grant numbers 96-2752-E-007-003-PAE, 97-2219-E-007-002, and 98-2213-E-007-016.

References


Author's personal copy

4229


4229


4229


4229