

**cpsc 499
assignment 1
kiranjit sidhu
230023668
14.11.2003**

contents

1	Introduction	3
2	BCMCS	4
3	MBMS	7
4	References	11

List of Tables

1	Abbreviations	2
---	-------------------------	---

List of Figures

1	Accounting in BCMCS (from the framework document)	5
2	Security in MBMS(from the framework document)	9

Format of the Paper:

The paper starts with a list of terms (Abbreviations) that have been used in the paper. An introduction section is included after that. This is followed by a Section on BCMCS and another one on MBMS. Each of these sections have subsections on the Core Network Element and other components of the service such as accounting and security framework. The internal structure of few of these sections has been kept similar to that of the framework documents (stage 2 in most cases). I have tried to describe the sections as I understood them myself after reading the documents. Finally, comparison has been done at various steps between the two methods and shown in separate Frames.

Abbreviations

Abbreviations used in this paper have been defined here.

Table 1: Abbreviations

Definition	Meaning
AAA	Authentication, Authorization and Accounting
BAK	Broadcast Access Key
BCMCS	Broadcast/Multicast Service
BM-SC	Broadcast Multicast Service Center
BSC	Base Station Controller
CBC	Cell Broadcast Center
CDMA	Code-division Multiple Access
CDR	Charging Data Record
GERAN	GSM EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
H-AAA	Home AAA
HLR	Home Location Register
MBMS	Multimedia Broadcast Multicast Services
MS	Mobile Station
PCF	Packet Control Function
PDSN	Packet Data Serving Node
PPP	Point to Point protocol
RNC	Radio Network Controller
SGSN	Serving GPRS Support Code
SMS	Short Message Service
UE	User Equipment
UTRAN	Universal Terrestrial Radio Access Network
WCDMA	Wideband Code-division Multiple Access

MBMS in CDMA2000 and BCBMS in WCDMA

1 Introduction

Wireless Telecommunications networks have been growing rapidly in the last few years. The services being offered by the networks have also been on the increase. Initially mobile technology was only being used for purpose of basic communication, but, with the advent of technologies such as CDMA2000 and WCDMA, this has all changed a great deal. Services like email, internet, SMS have all become immensely popular.

Broadcast and Multicast are two services which haven't quite yet reached their potential. Broadcast and Multicast are services by which providers can send information to multiple users at the same time. This information can be either text, audio or video streamed data. Users generally need to subscribe to multi cast group as it is considered to be closed group.

Broadcast and Multicast Services could become popular and thus, mobile network operators should be interested in MBMS/BCMSC. A few points have been discussed about why broadcast/multicast service might be a good trend:

- **Infrastructure**

As it primarily relies on infrastructure which already exists, the cost of starting up such a service is not going to be that great. Earlier it was not feasible as much because of not a lot of consumer interest, but now if introduced correctly it could be a great money making service for the mobile network operators.

- **Security Purposes:**

After the attacks in United States, US and the western world has become a lot more cautious about their national security needs. Broadcast services could be used as a tool for warning people of any such major security related issue.

- **Traffic/Sports:**

Broadcast/Multicast services could also target a huge target of consumers. In major metropolitan cities, where a lot of people get stuck in traffic jams during rush hour in the morning, this could be a great

asset. Also, for sports fan this could be an ideal way of knowing about score updates.

- **The Tech Generation**

The new generation is technology savvy. This can be seen by the examples set in Japan where a substantial portion of the consumers is the younger generation. This trend is quite similar to what is being seen here in North America as well. Thus providing new and useful services should be well accepted.

2 BCMCS

- **Core Network Element**

BCMCS Controller is the core network element that has been introduced in order to support this service. There are other entities, some of which are optional, that are used with the core element to provide BCMCS Service.

The primary purpose of the BCMCS controller is to manage the BCMCS session information. It can be used for authorization purposes by using the BCMCS Subscriber profile database which it can get from H-AAA via S-AAA. Another possible use of the BCMCS controller could be to facilitate the movement of the data from the content provider to the server.

A few other entities/components have been described here:

- Content Provider

This entity is used to provide the content that is to be broadcasted and/or multicasted.

- Content Server

This entity is mainly used for distribution of the content provided by the Content Provider to the Mobile Stations via packet data serving node. This is the last place where the contents can be modified or reformatted. The contents can be stored in the content server for transmission later on or they can be delivered to the its destination i.e. the mobile station via the PDSN.

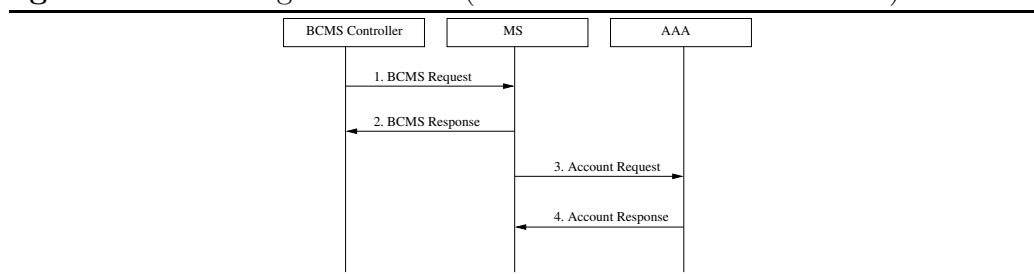
- AAA
It works for the main purposes of BCMCS authentication, authorization and accounting. It has access to the Subscriber Profile Database which it uses for authentication purposes. This information could possibly be passed on to the BCMCS Controller and authentication can be done there.
- Subscriber Profile Database
This is used to store user registration information.
- BCMCS Subscriber Profile Manager
This entity is used for updating information in Subscriber Profile Database.

• Accounting

The basic accounting model of the BCMCS is:

- Client logs on (or connects to the BCMCS Controller) and tries to get BCMCS information.
- This information is sent to the client by the controller.
- BCMCS controller updates accounting information by providing AAA with details of the BCMCS session.
- AAA sends back an acknowledgement once it has finished updating the information.

figure 1 Accounting in BCMCS (from the framework document)



To provide accounting functionality BCMCS has to gather some data which it can use for this purpose. Some of the important ones have been mentioned here:

Content Name (Name of the BCMCS Content requested), Type (video, audio, text) ,Volume of content sent, user id, mobile id, during what time of day was the service used and the BCMCS_Flow_ID (multiple records for same multicast ipflow).

One more topic is that of **Implications of Pre-paid Subscription** has been mentioned but not discussed at all in the framework documentation. I have tried to recommend a possible way to implement such a system.

- In case of pre-paid subscription system, on receiving a BCMCS request, the BCMCS controller can check with AAA to see if the current user requesting is a regular user or is a pre-paid user.
 - * If it is the case of a regular user then follow the steps as mentioned in the basic accounting model defined above.
 - * On the otherhand, if the user is a pre-paid one, then check to see if enough funds are available for the content that has been requested.
 - If so then provide information to the user and update AAA.
 - Else notify MS of lack of funds.

• Security

There are a few aspects of Security Framework that have been discussed here. In case of BCMCS, authentication and authorization needs to be done for purpose of retrieving content information and BCMCS registration. In the first case, authorization can be done using the subscriber's profile database by the BCMCS Controller from the HAAA which passes it on to SAAA and then to the BCMCS Controller.

For the case of BCMCS registration, there are two ways to do the authentication:

- Use PPP Sessions
 - BSC/PCF sends authorization request to PDSN.
 - PDSN has a PPP session with the mobile station.
 - AAA is then used for authentication purposes.
- Authorization Signatures

- * Signature is generated by the mobile station using the BAK (Broadcast access key) encryption key for the specific BCMCS program.
- * PDSN takes this signature and passes it on to the controller which in turn authenticates using AAA.

Encryption can also be provided if required. Mobile station should also be able to simulataneously use other services while receiving BCMCS data.

3 MBMS

MBMS introduces the concept of point-to-multipoint data transfer in WCDMA which had point-to-point initially.

- **Core Network Element**

Broadcast Multicast Service Center (BM-SC) is the core network entity that has been introduced to provide this service. In the case of BCMCS, few other existing network components will be used to provide some functionality.

- **Broadcast Multicast Service Center (BM-SC)**

The main functions of BM-SC is to manage transmission of data to the UE. It has to authorize and authenticate the content provider. It then checks the content and tests them for validity. It is also responsible for charging. BM-SC can either send the data over to the UE as it receives it or can chedule the delivery of the multi-cast/broadcast to some later time. Also 3rd party providers can be managed by the BM-SC as well.

Note: The core network entity in case of BCMCS, BCMCS Controller is not responsible for transferring data to the MS but in case of MBMS, BM-SC is responsible for doing that.

- **User Equipment (UE)**

User Equipment should be able to receive MBMS data without user request once the UE has been authorized. UE should be able

to receive other requests while receiving MBMS data. If data loss occurs then the MBMS applications deal with that.

- **UTRAN/GERAN**

This is used primarily for delivering the contents of MBMS efficiently to the multicast or broadcast area. By efficiently, we mean there should be no data loss and if data loss does happen then it should be able to deal with it. It is responsible for creating the point-to-multipoint channels for MBMS. Also it should be able to keep on handling other services while simultaneously handling a MBMS service request.

- **SGSN**

SGSN can be used to authenticate users based on subscription data from the HLR. It creates the CDR (Charging Data Record) for content provider and for each user. Other functions which are provided by SGSN can be modified and used with BM-SC for MBMS purposes.

- **GGSN**

This is used to create user planes for users who have requested access to the MBMS service. Tunnelling is one of the most important features of GGSN. BM-SC is able to transmit data to users roaming in a different network using GGSN.

- **CBC(Cell Broadcast Center)**

This is used to advertise MBMS services to the users.

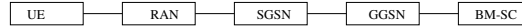
Few options are available for data transfer. In order to take the advantage of being able to send data to roaming users and to users in PMM idle state, BM-SC can send the data to SGSN either directly or through GGSN.

- **Security**

The AKA protocol is used to authenticate a user and to agree on the keys to be used between them in case of point-to-point services. These keys are then used for security purposes for user data between RNC and UE.

Note: BCMCS uses AAA for authentication, MBMS on the other hand uses AKA protocol.

figure 2 Security in MBMS(from the framework document)



Authentication and Authorizing Users

The user equipment and the network can authenticate each other using the AKA, similar to the case of point-to-point. Once authenticated, the user does not need to be rechecked again for accessing that multicast service.

Key Management and Distribution

BM-SC needs to manage keys separately as it will have a key for each service and will need to provide that key to multiple users of that service. BM-SC needs to change the keys frequently. It should change the keys every time a user activates a service and de-activates a service. This is because if a user comes in, we want to stop user from decrypting data being sent to user before user has physically joined the service. Similarly, on user leaving the service, we want to stop them from decrypting data.

Protection of Transmitted Data

There is a need for end to end security of data between the UE and the BM-SC. This is needed for data that is sensitive, BM-SC has to decide whether a given data is sensitive or not. Depending upon what type of data is being transmitted the actual method might differ i.e. for video it might be different from that of audio data.

- **Accounting**

There are few different categories that MBMS services can be charged for:

Broadcast Services

Multicast Services

- **Broadcast**

In case of Broadcast services we are only concerned with charging information for the content provider and not the users. For this purpose the BM-SC has to gather some data and it then generates a charging data record (CDR) for the billing of the content

provider. Some of the data that it needs to collect could be: volume of data being sent, time of day it is being sent and number of cells in the area that it is broadcasting the data in.

– **Multicast**

* Content Provider Charging

Again as in the case of broadcast, the billing is done by BM-SC. BM-SC uses CDR from SGSN and GGSN in this case and combines it with the CDR that it generates. Same kind of information needs to be collected as mentioned in the case of Broadcast charging scheme.

* Subscriber Charging

· Online Charging

CAMEL - This can be used to handle pre-paid services e.g. credit checking for online charging.

The CAMEL facility needs to be greatly extended for SGSN in order to achieve this.

Note: MBMS has defined CAMEL as the protocol for pre-paid services, where as BCMCS has yet to decide on a method for doing this.

· Offline Charging

This could be based on the actual volume of data received by the user or on the services that a user activated even if they did or did not utilize that service. If SGSN is in different network than the BM-SC, then SGSN needs to produce some information for the BM-SC to use in order for it to correctly generate the user charging statistics.

4 References

1. Multimedia Broadcast/Multicast Service (MBMS)
Architecture and functional description
Version: 6.0.0
Spec: 23.246
www.3gpp.org
2. Multimedia Broadcast/Multicast Service (MBMS)
Stage 2
Version: 6.1.0
Spec: 23.846
www.3gpp.org
3. 3G Security
Security of Multimedia Broadcast/Multicast Service (MBMS)
Version: 0.2.0
Spec: 33.246
www.3gpp.org
4. Broadcast/Multicast Services - Stage 1
Version: 1.0
Spec: S.R0030
http://www.3gpp2.org/Public_html/specs/S.R0030_v1.0.pdf
5. BCMCS Framework document
Version: 0.1.2
[ftp://ftp.3gpp2.org/TSGX/Working/2003/2003-07/BCMCS Adhoc 2007_08_03/](ftp://ftp.3gpp2.org/TSGX/Working/2003/2003-07/BCMCS%20Adhoc%202007_08_03/)