【DESCRIPTION】

【Invention Title】

# A CONDITIONAL ACCESS SYSTEM IN DIGITAL MULTIMEDIA BROADCASTING SYSTEM AND METHOD THEREOF

【Technical Field】

The present invention relates to a digital multimedia broadcasting (DMB) transmitting system. In particular, the present invention relates to a DMB transmitting system and method when a relay network other than a key network is built for a blanket area in a digital broadcasting system using a single frequency network (SFN).

【Background Art】

Digital broadcasting has characteristics of providing multiple channels, high quality, and multiple functions. In particular, development of multiplexing techniques has enabled concurrent combination of images, speech, and data irrespective of contents, size, and transmission thereof, and has formed a return channel through a modem to allow interactive services. Accordingly, digital data broadcasting has overcome the problems of conventional analog broadcasting and has provided multimedia services with high added value to viewers.

In general terrestrial and satellite digital broadcasting, a transmitter for respectively forming a key network or a relay network is provided in a single frequency network (SFN), a blanket area in which no service is received is generated in the key network or the relay network, and a relay or a gap filler is installed so as to cover the blanket area.

For example, in a satellite digital multimedia broadcasting (DMB) system, most regions are available for receiving signals from a satellite, and the gap filler is used to acquire a receiving region in blanket regions in which no direct signal receiving is possible, such as regions in a subway, a tunnel,

and a building. In other words, when it is not easy to directly receive satellite signals on a ground side, that is, within a tunnel, underground, and in a building, the gap filler receives the satellite signals through a satellite signal receive antenna and starts broadcasting.

Key centers represent broadcasting stations that function as a main center of the broadcasting network system, and they plan, produce, and transmit broadcast programs. In Korea, radio broadcasting stations include KBS, MBC, CBS, BBS, PBS, SBS, and Keukdong Broadcasting, and television broadcasting stations include KBS, MBC, and SBS. The broadcasting stations located in Seoul are established to be their transmitters.

Also, a relay center (RC) is an auxiliary station with less power and is also called a satellite station. Conventionally, a relay center has a service region, that is, a designated broadcasting region, but since boundary regions have weak radio wave arrival and blanket areas, the relay is installed for the boundary regions. The relay is installed at mountaintops for receiving radio waves from the key center, and it receives the waves through high-sensitivity receivers, electrically amplifies them, and broadcasts them as radio waves of different frequencies.

When a third service provider other than the broadcasting service providers with business rights participates in building and managing the broadcasting network or relay network, the service provider having entered the new business of building the network comes to acquire the right of using an additional broadcasting network or relay network, and it is required to control the service providers that do not join the business to not use the corresponding broadcast network or relay network or control them to optionally use the same. Also, it is needed to provide a subscriber with charged broadcast services on the corresponding broadcast network or relay network so that the subscriber may pay for the provision of services caused by usage of the network in the blanket area.

In other words, when a key center service provider is different from a relay service provider, the relay service provider generates the cost of

installing and maintaining a broadcast network in the shade region, and the relay service provider charges for the usage of the relay network. However, the relay service must be a charged service for the purpose of activating the relay network, but no appropriate treatment for the charged service has been provided up to now.

The above information disclosed in this Background section is only for enhancement of understanding of the background of the invention and therefore it may contain information that does not form the prior art that is already known in this country to a person of ordinary skill in the art.

【Disclosure】

【Technical Problem】

The present invention has been made in an effort to provide a DMB conditional access system and a conditional access method in the system having advantages of allowing general subscribers and extended service subscribers to conditionally access the key network and the relay network in the broadcast network having a single frequency network.

【Technical Solution】

In one aspect of the present invention, a transmission system for conditionally accessing digital multimedia broadcasting (DMB) according to transmitters includes: a key center system for scrambling a transmission stream by using a control word that is generated by using first transmitter identification information, encrypting the transmission stream, and transmitting encrypted broadcast signals having the first transmitter identification information through a key network; a relay system for receiving the encrypted broadcast signals from the key center system, inserting second transmitter identification information other than the first transmitter identification information into the encrypted broadcast signals, and transmitting the same, the second transmitter identification information being generated by the key center system from the first transmitter identification

information according to a predetermined matching algorithm; and an authentication system for receiving the matching key from the key center system, and transmitting the matching key to an extended service subscriber station that is available for a service provided by the relay system, the matching key being used to detect the first transmitter identification information from the second transmitter identification information.

In another aspect of the present invention, a transmission method for conditionally accessing digital multimedia broadcasting (DMB) according to transmitters includes a) generating a control word by using first transmission identification information for indicating that a transmitter is a key center; b) scrambling transmission streams including audio, video, and data provided by a plurality of contents providers by using the control word; c) encrypting the transmission stream scrambled in b), and ensemble multiplexing the transmission stream together with the first transmission identification information and the control word; and d) modulating the multiplexed broadcast signal into a transmission signal, and transmitting the same through a key network.

In still another aspect of the present invention, a transmission method for conditionally accessing digital multimedia broadcasting (DMB) according to transmitters includes: a) receiving encrypted broadcast signals from a key center, the encrypted broadcast signals including second transmitter identification information that is generated by the key center from first transmitter identification information that is the key center's identification information by using a specific matching algorithm; b) analyzing the received broadcast signals' second transmitter identification information, and inserting the second transmitter identification information other than the first transmitter identification information into the broadcast signals transmitted to a subscriber; and c) multiplexing/modulating the broadcast signals having the second transmitter identification information, and transmitting the broadcast signals to a subscriber station.

In still another aspect of the present invention, a system for

conditionally accessing digital multimedia broadcasting (DMB) according to transmitters includes: a transmitter identification information detector for detecting transmitter identification information from encrypted broadcast signals that are received through an antenna; a matcher for finding transmitter identification information of a key network corresponding to transmitter identification information detected by the transmitter identification information detector, and outputting a corresponding session key; a control word generator for generating a control word by using the session key generated by the matcher; a decoder for decrypting the received encrypted broadcast signals by using the control word generated by the control word generator; and a controller for decrypting the received encrypted broadcast signals by controlling the transmitter identification information detector, the matcher, the control word generator, and the decoder according to the broadcast network to which the transmitter determined by the transmitter identification information detected by the transmitter identification information detector belongs and according to the status whether the system is registered to an extended service.

In still another aspect of the present invention, a method for conditionally accessing digital multimedia broadcasting (DMB) in an extended service subscriber system includes: a) the extended service subscriber system receiving encrypted broadcast signals from a key center or a relay center; b) detecting transmitter identification information from a synchronization channel; c) checking whether the detected transmitter identification information is the key center's transmitter identification information; d) the extended service subscriber system externally receiving a matching key through the DMB network or a radio network when it is determined that the detected transmitter identification information is not the key center's transmitter identification information; and e) decrypting the received broadcast signals by using the matching key and the detected transmitter identification information

【Description of Drawings】

FIG. 1 shows a block diagram for transmitting encrypted broadcast signals in the single frequency network (SFN) according to an embodiment of the present invention.

FIG. 2 shows a DMB conditional access transmitting system according to an embodiment of the present invention.

FIG. 3 shows a block diagram for transmission of encrypted broadcast signals by a key center, a relay center, an authentication system, and a subscriber station according to an embodiment of the present invention.

FIG. 4 shows a DMB conditional access transmitting service according to an embodiment of the present invention.

FIG. 5 shows encrypted broadcast signals between the key network and the relay network according to an embodiment of the present invention.

FIG. 6 shows transmitted signals for respective channels of the key network and the relay network according to an embodiment of the present invention.

FIG. 7 shows transmitter identification information and control words that are transmitted by a key center transmitter through a synchronous channel according to an embodiment of the present invention.

FIG. 8 shows a key table for storing session keys that correspond to IDs by the key center transmitter according to an embodiment of the present invention.

FIG. 9 shows a flowchart of a method for transmitting encrypted broadcast signals in a key center system according to an embodiment of the present invention.

FIG. 10 shows a flowchart of a method for transmitting encrypted broadcast signals in a relay system according to an embodiment of the present invention.

FIG. 11 shows a condifuration diagram for a subscriber station of a DMB conditional access system for a transmitter according to an embodiment of the present invention wherein the subscriber station can be a private use

terminal or a mobile phone.

FIG. 12 shows a flowchart for a DMB conditional access method for a transmitter in a general subscriber station according to an embodiment of the present invention.

FIG. 13 shows a flowchart for a DMB conditional access method for a transmitter in an extended service subscriber station according to an embodiment of the present invention.

【BEST MODE】

An exemplary embodiment of the present invention will hereinafter be described in detail with reference to the accompanying drawings.

An encryption broadcast signal transmitting system and method thereof according to an embodiment of the present invention will now be described in detail, referring to the drawings.

In the terrestrial and satellite digital broadcasting system according to an embodiment of the present invention, it is controlled for a general subscriber or an extended service subscriber to differently use at least two networks in the broadcast network having a single frequency network so that one user may use all the networks and another user may use some networks by using a conditional access function.

In detail, the transmission stream that is transmitted to the subscriber is scrambled according to the control word, and transmitter identification information (TII) is applied as a value for finding the decoding of the transmission stream to thus perform a conditional access for the respective transmitters. Here, the TII is a proper identifier assigned to the transmitter, the TII signal is transmitted to a synchronous channel, and the TII can be used together with frequency information (FI) within the single frequency network (SFN).

As to the DMB conditional access system and the conditional access method in the system according to the embodiment of the present invention, a general conditional access system (CAS) will be described, and the difference

between the general CAS and the CAS according to the embodiment of the present invention will be described.

The CAS has been developed to protect various multimedia data transmitted to the subscriber station from a plurality of program providers, and to allow authenticated subscribers to access the data.

The CAS is a system for allowing registered users to receive specific broadcast signals or programs by introducing the subscriber concept to the general broadcasting so that each digital broadcast receiver may determine whether to supply a specific broadcast program to a receiving person. In the CAS, the transmitter transmits encrypted program signals and an entitlement assigned to each receiving person or a specific group, and the receiver allows the registered subscribers to decrypt the encrypted signals by using a decryptor (e.g., a smart card) attached to the receiver and then receive a program. In this instance, the authentication system provides a decryption key other than the smart card to the extended service subscriber in the embodiment of the present invention.

The transmitter of the CAS includes a subscriber management system (SMS), a scrambling engine, and an encryption engine. The subscriber management system (SMS) manages subscriber information, the scrambling engine scrambles the program so that no unregistered user may receive the transmission stream that is the programs, and the encryption engine encrypts entitlement control information.

Further, the receiver of the CAS includes an integrated receiver/decoder (IRD), an entitlement management message (EMM) authenticator, an entitlement control message (ECM) authenticator, and a transmission stream block, and it uses a customer ID key in the decryptor of the IRD to decrypt the service within the EMM regarding whether to have an entitlement and decrypts the control word (CW) within the ECM and thus receives the program.

Accordingly, the CAS requires the following functions. That is, the CAS needs a scrambling and descrambling function for protecting the original

signals against users who are not authorized to receive a commercial service, an entitlement control function for allowing the charged subscribers to have the signals analyzed, and an entitlement management function.

The scrambling process scrambles the multimedia data to be transmitted according to a predefined rule so that no user without entitlement may view the data, and in general, the signals are converted by using a control word (CW.)

In other words, the scrambling process changes the original broadcast signals so that no registered user may view them, and the scrambling process is variable depending on the broadcast program types (audio/video/data) and the signal types (analog/digital.)

The descrambling process is performed by the receiver that has the control word (CW) that is a descrambling key.

Also, the encryption process protects the control word (CW) that is transmitted together with the scrambled signals to be transmitted by the receiving user's decryptor, and the descrambling process can be accurately performed when the transmitter and the receiver have the same secret key.

In detail, the entitlement control function encrypts the control word (CW) so that it may be loaded in the ECM and then transmitted to a subscriber station, it is periodically transmitted for the purpose of security, and a new control word is encrypted for each period. The ECM includes a control parameter in addition to the encrypted control word (CW), the transmitter transmits the ECM to the subscriber station, and a microprocessor in the subscriber station compares an installed authorization parameter with the transmitted control parameter. When the comparison result shows that the parameters correspond to each other, the receiver is authenticated, and the control word (CW) that is the descrambling key is decrypted by using a decoding key that is received for each subscriber station. The control word (CW) has a different value for each program, and is changed periodically.

Also, the entitlement management function provides an entitlement to the subscriber station or updates the same, and the subscriber management

system generates an EMM and encrypts the EMM, and transmits the encrypted EMM to the receiver through a transmission stream. In this instance, the EMM functions to provide an entitlement to the decryptor of the receiver or update the entitlement.

In the embodiment of the present invention, identification of broadcast networks and the terminal's subscription to the extended service are distinguished. The network identification function (NIF) uses the transmitter identification information (TII) of the terrestrial DMB standard (ETS 300.401 of the Eureka-147 Rule) to assign identifiers to the broadcasting network and the relay network, and efficiently manages the networks according to distinguished signals. Therefore, in the embodiment of the present invention, transmission data are scrambled by using the control word (CW) and are then encrypted by using TII to thereby prevent access in the data level and provide security.

Here, the scrambling process is performed in order to prevent the terminal having no network identification function from being used with no fee for all the networks without the operation of identifying the network, and in this instance, the scrambling process is not applied to the relay network because the signals of the relay network are different from those of the key network and the scrambled signals of the relay network function as interference in the area of the overlapped signals.

Also, in the broadcast network having the single frequency network, general subscribers and extended service subscribers can receive services within the coverage of the key network, and the extended service subscribers can receive services within the coverage of the relay network. Further, the general subscribers and the extended service subscribers can receive services in the overlapped coverage of the key network and the relay network. In this instance, it must be basically assumed that the service provided to the general subscribers in the key network may not be influenced by an addition of a relay network, no reduction on the service coverage of the key network may be allowed, and service continuity may be generated by an handoff

generated between the key network and the relay network.

Referring to drawings, a DMB conditional access system and a conditional access method in the system according to an embodiment of the present invention will now be described.

FIG. 1 shows a method for transmitting encrypted broadcast signals in the single frequency network according to an embodiment of the present invention.

Referring to FIG. 1, when a key network 10 or a relay network 20 forms a single frequency network, a key center 11 of the key network 10 receives video, audio, and data from a plurality of program services providers and encrypts them, and inserts transmitter identification information (TIIa) for identifying the key network thereto to transmit encrypted broadcast signals. In this instance, the encrypted broadcast signals are passed through a DMB broadcasting station 12 including a DMB system and are transmitted to a relay center (RC) 21 from a transmission center (TC) 13 through the key network, or they are transmitted to the relay center 21 from the key center 11 through a private line. In this instance, when the broadcast signals are transmitted to the relay center 21 from the key center 11, the key center 11 converts the TIIa into TIIb by using a specific matching algorithm to insert the TIIb other than the TIIa into the broadcast signals and transmit them to the relay center 21. The TIIa is provided to the key center 11 by an authentication system 230. Also, the encrypted broadcast signals within the key network 10 are transmitted to a subscriber station 14 in the key network 10.

In the relay network 20, the relay center 21 receives the encrypted broadcast signals through the key network or a private line and transmits the same to the relay 21 in the blanket area through a relay link, and a gap filler in the blanket area transmits them to a subscriber station 23 within the relay network.

Accordingly, as to the encrypted broadcast signals in the single frequency network, the key network 10 or the relay network 20 transmits TII

for identification of networks, and subscriber stations 14 and 23 within the key network 10 or the relay network 20 respectively decrypt and reproduce the encrypted broadcast signals according to different schemes.

FIG. 2 shows a schematic diagram of a DMB conditional access transmitting system according to an embodiment of the present invention.

Referring to FIG. 2, the DMB conditional access transmitting system includes a key center system 210, a relay system 220, and an authentication system 230, and the system transmits the encrypted broadcast signals to the subscriber station 240. The key center system 210 will now be used to represent the key center and the relay system 220 will be used to indicate the relay center.

The key center 210 scrambles transmission streams by using a control word (CW), generates transmitter identification information (TIIa) of the key center to encrypt the control word by using the TIIa of the key center and thereby protect the control word (CW), and transmits the encrypted broadcast signals through the key network. The key center 210 establishes the TIIa of the key center and applies the TIIa so as to protect the control word that is a scrambling key, and it also periodically changes the TIIa of the key center 210 and periodically applies the TIIa that is changed by the performance of encryption.

In further detail, the key center 210 generates a control word for scrambling the transmission stream by using a session key corresponding to TIIa through a specific key table (refer to FIG. 8) storing a session key corresponding to TIIa and generates broadcast signals with the encrypted control word that is an entitlement control message (ECM), and transmits them. Referring to FIG. 8, the key center 210 stores a key table showing session keys ($SK_{TII_{a1}}, \cdots, SK_{TII_{a10}}, \cdots, SK_{TII_{aN}}$) corresponding to a plurality of key center identification numbers ($TII_{a_1}, \cdots, TII_{a_{10}}, \cdots, TII_{a_N}$) in a predetermined memory. For example, when the identification number of the key center 210 is given as $TII_{a_1}$, the corresponding session key is $SK_{TII_{a1}}$, and the session

key $SK_{TII_{ai}}$ is used to generate a control word and apply the control word to the scrambling process.

In the case of transmitting the broadcast signals to the relay center 220, the key center 210 changes TIIa of the key center into TIIb, and relays the broadcast signals with the inserted TIIb to the subscriber station and the relay in the blanket area. In this instance, the key center 210 receives TIIb from the authentication system 230 and uses it in a like manner of the TIIa, and the authentication system 230 controls to make TIIa corresponding to TIIb be known when TIIa is changed to TIIb according to a predetermined matching algorithm and a corresponding matching key is subsequently used.

The relay center 220 amplifies signals of the key network corresponding to the single frequency network and transmits the same, or modulates and amplifies the streams input by the key center 210 through a private line and transmits them. A relay network server (not shown) in the relay center 220 gathers transmission signals of six service providers to generate TII, modulate the signals according to the TDM scheme, and then transmit the same through a satellite station so as to relay broadcast programs.

The authentication system 230 generates TIIa and TIIb to the key center 210, and transmits a matching key for identifying TIIa that is the identifier of the key center 210 from TIIb that is the identifier of the relay network to the extended service subscriber station. In this instance, the matching key can be periodically updated by the key center 210.

In detail, the key center 210 includes a service multiplexer 212, a scrambler 213, a transmitter identification information (TIIa) generator 215, an encryptor 214, a system multiplexer 216, a modulator 217, and a transmitter 218.

The service multiplexer 212 multiplexes the audio, video, data, and additional information respectively provided by a plurality of contents providers into transmission streams. The audio, video, and data are provided by a plurality of contents providers through a video encoder 211a, an

audio encoder 211b, and a data server 211c, respectively. In this instance, the audio service is transmitted through an independent channel so as to provide a CD-quality audio service. The data service is used for transmission of text data such as lyrics of the audio service. The video service is generated into a single stream by a video multiplexer, and is then transmitted since the video service includes motion pictures, audio, and multiplexing/synchronization information. In this instance, the audio, data, and video service are multiplexed into a service channel by the service multiplexer 212, the service channel is then combined with transmission data to be a single frame by the system multiplexer 216, and the frame is transmitted through a physical channel.

The scrambler 212 scrambles the multiplexed transmission streams according to a predetermined rule by using a control word (CW) so that any user who has no entitlement may not receive transmission streams.

The transmitter identification information (TIIa) generator 215 generates TIIa for indicating that the transmitter transmitting broadcast signals is the key center. In this instance, the transmitter identification information (TIIa) generator 215 directly generates TIIa, and it is desirable to receive the TIIa generated by the authentication system 230 and use the same.

The encryptor 214 generates an ECM having an encrypted control word (CW) by using a session key corresponding to TIIa of the key center so as to protect the control word (CW).

The system multiplexer 216 multiplexes encrypted broadcast signals together with system control data into a single ensemble transmission stream. The system multiplexer 216 is also called an ensemble multiplexer, and in this instance, a plurality of audio compression streams and various types of data are respectively channel encoded and are then multiplexed together with the system control data into a single transmission stream, and the above-noted multiplexed result is called an ensemble.

The modulator 217 modulates the ensemble multiplexed broadcast

signals into transmission signals.

The transmitter 218 transmits the encrypted broadcast signals including the TIIa and the control word (CW) to the subscriber or transmits the broadcast signals including the TIIb to the relay center 220.

Also, the relay center 220 includes a transmitter identification information (TIIb) inserter 221, a multiplexer/modulator 222, a relay center transmitter 223, a gap filler (GF) transmitter identification information (GF TIIb) generator 224, a GF multiplexer/modulator 225, and a GF transmitter 226.

The TIIb inserter 221 analyzes TIIb in the encrypted broadcast signals received from the key center 210 and inserts TIIb into the broadcast signals that are transmitted to the subscriber so as to indicate that the transmitter transmitting the broadcast signals is a relay center, through a relay network.

The multiplexer/modulator 222 multiplexes and modulates the signals that are output by the transmitter identification information inserter 221 of the relay center. In this instance, the multiplexer/modulator 222 can be divided into a multiplexer and a modulator and then can be installed.

The relay center transmitter 223 transmits the multiplexed and modulated broadcast signals to the subscriber station, or transmits the same to the gap filler through a relay link.

The GF TIIb generator 224 generates GF TIIb.

The GF multiplexer/modulator 225 changes the TIIb in the encrypted broadcast signals received from the relay center into GF TIIb, and then multiplexes and modulates the GF TIIb.

The GF transmitter 226 transmits the multiplexed and modulated broadcast signals to the subscriber station in the blanket area.

The authentication system 230 includes a user authentication server 231 which periodically transmits a matching key so that the subscriber station may decrypt the received key and may extract a corresponding control word. In detail, the user authentication server 231 transmits a matching key to the extended service subscriber station through a wireless network when the

extended service subscriber station has a wireless modem, or it transmits a matching key to the extended service subscriber station through a digital multimedia broadcasting (DMB) network when the extended service subscriber station has no wireless modem.

Also, the subscriber station 240 can be a general subscriber terminal or an extended service subscriber terminal, and the general subscriber or the extended service subscriber can view broadcasting programs irrespective of the above-noted encryption in the key network, and the extended service subscriber having registered to the service can view the broadcasting programs by using the matching key transmitted from the authentication system 230. The configuration and operation of the subscriber station 240 will be described later with reference to FIG. 11.

In the embodiment of the present invention, in the case of the single frequency network, data of the key network and the relay network have the same streams, and their signal synchronization is guaranteed so that the broadcast network is configured without interference between the key network and the relay network. In this instance, TII is used as transmitter identification information. Substantially, TII is used for the subscriber station to identify whether the broadcast signals are transmitted through the key network or the relay network. In this instance, no interference of the single frequency network is generated when TII has different pieces of transmitter identification information. TII is not provided in the data region, but is established by combining carriers of an OFDM synchronous channel, and the combinations are arranged without iteration so that the received transmitter ID can be identified without receiving at least two signals from the single frequency network.

FIG. 3 shows a block diagram for transmission of encrypted broadcast signals by a key center, a relay center, an authentication system, and a subscriber station according to an embodiment of the present invention.

Referring to FIG. 3, when the key center 210 transmits TIIa of the key center, a control word (CW), and encrypted broadcast signals to the

subscriber station 240a in the key network, the subscriber station 240a including the general subscriber station and the extended service subscriber station decrypt the encrypted broadcast signals and then reproduce them by using the TIIa and the control word (CW). Also, the key center 210 transmits key center identification information (TIIa) to the authentication system 230 through a synchronous channel, transmits relay center identification information (TIIb) to the relay center 220, and transmits an entitlement control message (ECM)/entitlement management message (EMM) through a fast information channel (FIC).

As to the relay network, when the relay center 220 inserts the relay center's TIIb into the broadcast signals and transmits them to the subscriber station 240b, the subscriber station 240b that is a general subscriber station cannot decrypt the encrypted broadcast signals by using TIIb, and the subscriber station 240b that is an extended service subscriber station can know TIIa that corresponds to TIIb by receiving a matching key from the authentication system 230 and can obtain a session key for decrypting the control word and accordingly can decrypt the encrypted broadcast signals and reproduce the broadcast signals. That is, in the relay network, the relay center 220 transmits the relay center's TIIb and encrypted broadcast signals to the subscriber station 240b, and transmits the ECM/EMM to the authentication system 230. In this instance, the extended service subscriber station receives the matching key through a corresponding wireless network when the extended service subscriber station has a wireless modem, and it receives the matching key through the DMB network and decrypts the encrypted broadcast signals when it has no wireless modem.

FIG. 4 shows a DMB conditional access transmitting service according to an embodiment of the present invention.

Referring to FIG. 4, a DMB conditional access service area according to an embodiment of the present invention includes a key network 310, a relay network 320, and an area 330 in which the key network coverage and the relay network coverage are overlapped.

A key network transmitter 311 is provided in a key network 310, and a subscriber station receives a key center TIIa and a control word from the key network transmitter 311 to thus receive broadcast signals.

A relay center 321 is provided in a relay network 320, and extended service subscriber stations 322 and 323 receive encrypted broadcast signals with relay center TIIb inserted thereinto from the relay center 321. In this instance, the extended service subscribers 322 and 323 in the relay network 320 can receive broadcast signals and the general subscribers cannot receive the same since the subscribers 322 and 323 receive the ECM/EMM and the matching key from the user authentication server 231 through the DMB network or the wireless network.

Also, the subscriber station 331 receives the key center TIIa from the key network transmitter 311 or the relay center TIIb from the relay center 321 in the area 330 wherein the key network coverage and the relay network are overlapped.

FIG. 5 shows encrypted broadcast signals between the key network and the relay network according to an embodiment of the present invention.

Referring to FIG. 5, transmission of the encrypted broadcast signals in the T-DMB key network 410 is performed as follows.

When video 412a, audio 412b, and data 412c are provided from a plurality of program providers, they are multiplexed into transmission streams by the service multiplexer 414, and the multiplexed transmission streams are scrambled by the scrambler 413 by using a control word.

The control word is encrypted by the session key that corresponds to the TIIa inserted by the TIIa generator 415, the encrypted control word is multiplexed by the system multiplexer 416, and the multiplexed control word is transmitted by the key network transmitter 411. In this instance, TIIa is provided at the header of the data structure of the encrypted broadcast signals, and the scrambled transmission streams including the video 412a, audio 412b, and data 412c are provided at the body of the data structure.

The process for receiving the encrypted broadcast signals in the

T-DMB relay network 420 will now be described.

The broadcast signals transmitted by the key network transmitter 411 are received through the relay center 421, and in this instance, the relay center's TIIb inserter 422 inserts the TIIb transmitted by the key network transmitter 411 by the operation of the multiplexer/modulator 423, and in this instance, the TIIa at the header is changed into TIIb, and the video, audio, and data are transmitted as broadcast signals that are originally transmitted from the key center.

That is, when transmission streams are scrambled by using a control word, a TII value is inserted into a synchronous channel, and this signal is transmitted to the relay network, TIIa of the synchronous channel is changed into TIIb, and the data are transmitted as they are in the relay network. Therefore, no interference occurs between the data when the data are received within a specified area in the SFN since the data are the same as each other, and different TII values can be detected in the overlapped area of the key network area and the relay network area since the synchronous channel identifies different values.

Therefore, the general subscriber can receive TIIa that is received by the key network and cannot receive relay center TIIb from the relay network since the relay center TIIb is transmitted in the relay network in a different manner of the key center TIIa, and also, the extended service subscriber can receive TII in the key network, and can reproduce the encrypted broadcast signals when receiving a matching key for detecting TIIa through the DMB network or the wireless network.

In other words, the general subscriber station can receive the TIIa value of the key center, and the extended service subscriber station that is available for the relay network performs a similar operation as that of the general subscriber in the key network and receives a relay center TIIb value and a matching key through another network in the relay network. In this instance, the other network is a DMB network or a wireless network, and when a terminal has no wireless modem, in a like manner of a vehicle type

terminal or a private-use receiver depending on the terminal types, the terminal receives a matching key through the DMB's fast information channel (FIC) and then decrypts signals.

When having a wireless modem, the terminal receives the matching key through the corresponding wireless network. A general subscriber can receive a TIIa value from the key center network and he cannot receive signals in the relay network when failing to additionally receive a matching key for decryption from the relay network, and a relay network extended service subscriber can receive signals in the key network and can receive them by using the matching key that is received through the above-noted network in the relay network. In this instance, the fast information channel (FIC) transmits the same ECM and EMM as those of the relay network in the key network area since signals are not damaged when the key network corresponds to the relay network.

The problem that occurs in the above description is that the general subscriber can receive signals in the relay network when he stores the TIIa that is received in the key network and then moves to the relay network. To solve the problem, an encryption server in the key center periodically modifies the key center TIIa, and applies the modified TIIa to the process for scrambling the transmission streams.

Further, when the key network's TIIa has a CW, errors may occur in the mobile condition and the received signal cannot be accurately decrypted, and hence, some bits of the symbol of the TII can be used as a error correction code (ECC) so as to more accurately correct the errors.

FIG. 6 shows transmitted signals for respective channels of the key network and the relay network according to an embodiment of the present invention.

Referring to FIG. 6, key center TIIa and a control word 512 are alternately transmitted to the synchronous channel (SC) 511 in the key network area 510, and an ECM and an EMM that are encryption information are transmitted to the fast information channel (FIC) 513 so as to decrypt the

received data. Also, relay center's TIIb is transmitted to the synchronous channel 521 of the relay network 520 so as to identify the relay network, and an ECM and an EMM 524 that are encryption information are transmitted to the FIC 523 so as to decrypt the received data.

In detail, a transmission frame according to an embodiment of the present invention includes a synchronization channel (SC), a fast information channel, and a main service channel (MSC.)

The synchronization channel includes a null symbol and a phase reference symbol (PRS), and a TII signal is provided to the null symbol. The synchronization channel includes information required for a transmission mode, a symbol, and frequency synchronization. Also, the synchronization channel is used for frame synchronization, carrier frequency synchronization, channel estimation, and default demodulation functions.

The fast information channel (FCI) includes service information (SI), a fast information data channel (FIDC), multiplex configuration information (MCI), and a conditional access (CA.)

The MCI of the FIC is used to be transmitted to a receiver part as information such as a service type, a location, and a pattern, and then to analyze the MSC. In this instance, the SI includes a service title and channel information.

FIG. 7 shows transmitter identification information and control words that are transmitted by a key center transmitter through a synchronous channel according to an embodiment of the present invention.

Referring to FIG. 7, the method for transmitting the key center's transmitter identification information and a control word (CW) through a synchronization channel in the key network is illustrated. Generally, the control word (CW) has 64 bits, and in this instance, when a frame range transmittable together with transmitter identification information TIIa is 8 bits, a 64-bit control word (CW) is divided into an 8-frame synchronization channel and are then transmitted. When the control word (CW) is transmitted, key center transmitter identification information TIIa for identifying the key center

is transmitted. In this instance, the reference numerals 610a, 610b, and 611a to 611n indicate synchronization channels (SC), the reference numerals 620a and 620b show key center transmitter identification information TIIa, and the reference numerals 630a to 630n are control words (CW1, CW2, ···, CWn) that are transmitted for the respective synchronization channels.

FIG. 9 shows a flowchart of a method for transmitting encrypted broadcast signals in a key center system according to an embodiment of the present invention.

Referring to FIG. 9, in the method for transmitting encrypted broadcast signals in a key center system, the service multiplexer 212 of the key center multiplexes the audio, video, and data provided by a plurality of contents providers into transmission streams (S101).

Next, the TIIa generator 215 generates TIIa (S102), finds a session key (SK) corresponding to the TIIa from a key table to generate a control word (CW) (S103). The scrambler 213 scrambles the service multiplexed transmission stream by using the control word (S104.)

The encryptor 214 encrypts the broadcast signals scrambled in the step S104, inserts the control word and the TIIa thereinto, and outputs them, and the system multiplexer 216 ensemble multiplexes the signals output by the encryptor 24 and corresponding information (S105.) The system multiplexer 216 generates ECM/EMM and multiplexes the same with the encrypted broadcast signals.

Next, the system multiplexer 216 modulates the multiplexed broadcast signals into transmission signals (S106,) and transmits the modulated broadcast signals to the subscriber station or the relay center (S107). In this instance, when the receiver is the relay center, relay center transmitter identification information (TIIb) other than the key center transmitter identification information (TIIa) is inserted into the broadcast signals, which are then transmitted.

Next, the key center checks a predetermined period (S108), modifies key center transmitter identification information (TIIa) for each period (S109),

and encrypts the broadcast signals by applying the modified TIIa (S110). Therefore, the above-described steps S105 to S110 are repeated for each period.

FIG. 10 shows a flowchart of a method for transmitting encrypted broadcast signals in a relay system according to an embodiment of the present invention.

Referring to FIG. 10, in the method for transmitting encrypted broadcast signals in a relay system, the relay center receives the above-noted encrypted signals from the key center through a key network or a private line (S201). In this instance, since the broadcast signals received from the key center to the relay center has relay center transmitter identification information (TIIb) inserted thereinto, the relay center analyzes the broadcast signals (S202) and insert TIIb into the broadcast signals transmitted to the relay network (S203).

Next, the relay center multiplexes/modulates the relay center TIIb inserted broadcast signals (S204), and then transmits them to the subscriber station through a relay center transmitter (S205).

In this instance, when the subscriber station is located in the blanket area (S206), the relay center transmits the broadcast signals to the gap filler (GF) within the blanket area through a relay link (S207). Substantially, the broadcast signals are transmitted concurrently to the GF and the subscriber station.

Next, the GF generates GF TIIb (S208), and modifies the TIIb transmitted by the relay center into GF TIIb (S209). In this instance, the reason for identifying the relay center TIIb and the GF TIIb of the GF in the blanket area is that a plurality of relay centers can be formed and a plurality of blanket areas can be formed in each relay center, and for example, it is needed to identify GF TIIb of the relay center in each blanket area when the blanket areas are overlapped.

The broadcast signals into which the modified GF TIIb is inserted are multiplexed/modulated (S210), and are transmitted to the subscriber station

through the GF transmitter (S211).

FIG. 11 shows a condifuration diagram for a subscriber station of a DMB conditional access system for a transmitter according to an embodiment of the present invention wherein the subscriber station can be a private use terminal or a mobile phone.

Referring to FIG. 11, a subscriber station 800 of the DMB conditional access system includes a transmit/receive antenna 810, an RF module 820, a TII detector 830, a decoder 840, a controller 850, a matcher 860, a control word generator 870, and a display 880, and can further include a wireless modem 890.

On receiving encrypted RF broadcast signals through the antenna, the RF module 820 selects a corresponding channel and converts the received broadcast signals into digital signals to be output.

The TII detector 830 detects a TII value that is transmitter identification information from among the broadcast signals output by the RF module 820, and outputs the TII value.

The matcher 860 has a matching algorithm program for finding transmitter identification information by using a matching key. That is, the matcher 860 has a matching function in a program format for extracting the TII value of the key center corresponding to the TII value detected by the TII detector 830, and detect TIIa that is the key center's transmitter identification information through the above-noted matching algorithm. Also, the matcher 860 matches the session key that corresponds to the TIIa that is the key center's transmitter identification information with a value of a key table that corresponds to the key table shown in FIG. 8, and then outputs the matched value.

The control word generator 870 generates a control word by using the session key output by the matcher 860.

When the signals output by the RF module 820 are encrypted broadcast signals, the decoder 840 decrypts the broadcast signals by using the control word generated by the control word generator 870 and outputs the

decrypted broadcast signals, and the display 880 displays video data decrypted by the decoder 840.

The controller 850 controls the whole operation of the subscriber station 800, and in particular, it identifies the TII value detected by the TII detector 830, and when the transmitter for the broadcast signals is determined to be a relay center according to the identified TII value, the controller 850 transmits a TII value to the matcher 860 so as to identify TIIa that is the key center's transmitter identification information corresponding to the TII value, and transmits a control word to the decoder 840 so that the control word generated by the control word generator 870 may be used by the decoder 840. In this instance, the matching can be given when the subscriber station is an extended service subscriber's. That is, the general service subscriber who is within the relay network is not allowed to receive a matching key so that he cannot decrypt the encrypted broadcast signals and is controlled not to receive DMB signals.

The matcher 860 has programs of a matching algorithm for finding transmitter identification information by using a matching key and a matching algorithm for foinding a session key corresponding to transmitter identification information. That is, the matcher 860 a program for a matching function for extracting a TIIa value that is the key center's transmitter identification information corresponding to the TII value detected by the TII detector 830 and a program for a matching function for extracting a session key that corresponds to the TIIa value, and the matcher 860 finds the TIIa and the session key through the matching algorithms.

Further, when the subscriber station 800 is a private use terminal without the wireless communication modem 800, it receives a matching through the DMB network. Also, when the subscriber station 800 is a mobile phone having a wireless modem 880, it wirelessly receives a matching key through a radio network by the authentication system, and in this instance, the matching key is encrypted by using a proper number of the subscriber station 800 to thus control the corresponding matching key to be descrypted in the

corresponding subscriber station and prevent hacking.

Referring to FIG. 12, a DMB conditional access method for a transmitter in a general subscriber station according to an embodiment of the present invention will be described.

When a key center or a relay center (or a relay in a blanket area) transmits encrypted broadcast signals, the general subscriber station 800 receives the encrypted broadcast signals from the key center or the relay center through the transmit/receive antenna 810 and the RF module 820 (S301.) Also, the general subscriber station 800 detects TII transmitted together with the broadcast signals through the synchronization channel (SC) (S302.)

Next, the controller 850 checks whether the TII that is transmitted together with the encrypted broadcast signals and is then detected by the TII detector 830 is TIIa that is the key center's transmitter identification information (S303.) In this instance, the encrypted broadcast signals that are received from the key center include TIIa and a control word, and the encrypted broadcast signals that are received from the relay center include TIIb.

When the detected TII is the key center's TIIa, the decoder 840 descrambles the encrypted broadcast signals by using the control word that is provided in the broadcast signals (S304), and displays the same on the display 870 (S305.)

In this instance, the above-described steps S303 to S305 are repeated since the TIIa and the control word are modifies for each predetermined period.

When the TII is not the key center's TIIa in the step S903, that is, when the TII is the relay center's TIIb, a value of the counter installed in the general subscriber station is increased (S306) to satisfy the case in which the general subscriber station is provided in a key network and is then moved to a relay network through an overlapped network.

Next, it is checked whether the value of the counter is the

predetermined period (S307) and the step S307 is repeated for the period, that is, when a time is passed.

When the counter value corresponds to the predetermined period, the counter is controlled to be reset, and the general subscriber station's receiving of the encrypted broadcast signals is restricted (S308.)

When the general subscriber station is provided in the relay network from the start, the encrypted broadcast signals are conditionally accessed from the start irrespective of the value of the counter. Therefore, the access to broadcasting is controlled within the relay network when the subscriber station is not an extended service subscriber station that is registered to a service available for encrypted broadcast signals.

Referring to FIG. 13, a DMB conditionall access method of an extended service subscriber station for a transmitter according to an embodiment of the present invention will now be described.

When a key center or a relay center (or a gap filler in the blanket area) transmits encrypted broadcast signals, the extended service subscriber station 800 receives the encrypted broadcast signals through the transmit/receive antenna 810 and the RF module 820 (S401.) The TII detector 830 detects TII that are transmitted together with the broadcast signals from the synchronization channel (SC) (S402.) In this instance, TII can be detected in the synchronization channel (SC.)

Next, The TII that are transmitted together with the encrypted broadcast signals is detected by the TII detector 830, and the controller 850 checks whether the detected TII is TIIa of the key center (S403.) In this instance, TIIa and a control word are included in the encrypted broadcast signals received from the key center, and TIIb is included in the encrypted broadcast signals received from the relay center,

When the detected TII is the key center's TIIa, the decoder 840 descrambles the encrypted broadcast signals by using the control word included in the broadcast signals (S404) and displays them on the display 870 (S405.)

In this instance, the TIIa and the control word (CW) are modified by the key center for each predetermined period, and hence, the above-noted steps S403 to S405 are repeated.

When the TII is not the key center's TIIa in the step S403, that is, when the TII is the relay center's TIIb, the extended service subscriber station 800 receives a matching key for detecting the key center's TIIa from the authentication system through the DMB network or the wireless network (S406.) As described above, when the extended service subscriber station 800 has a wireless modem 880, it receives the matching key through the wireless network, and when it has no wireless modem, it receives a matching key in the ECM/EMM format through the DMB network.

Therefore, the matcher 860 of the controller 850 detects TIIa corresponding to TIIb by using the matching key (S407) and detects a session key corresponding to the detected TIIa (S408.)

When the control word generator 870 generates a control word by using the session key that is detected in the step S1007 (S409,) the decoder 840 receives the control word and uses the same to descramble the encrypted broadcast signals (S404) and displays them on the display (S405.)

As described above, referring to FIG. 9 to FIG. 13, when an extended service subscriber station is located within the relay network, the above-noted authentication system transmits a matching key for decrypting the encrypted broadcast signals according to a request by the extended service subscriber station. As described above, when the general subscriber station is provided in the relay network area, the subscriber station's receiving state is restricted by the encrypted broadcast signals, access is restricted by the encrypted broadcast signals, and the general subscriber station is to be exchanged with an extended service subscriber station in order to cancel the restriction, and the encrypted broadcast signals are decrypted when receiving the matching key from the authentication system.

While this invention has been described in connection with what is presently considered to be practical exemplary embodiments, it is to be

understood that the invention is not limited to the disclosed embodiments, but, on the contrary, is intended to cover various modifications and equivalent arrangements included within the spirit and scope of the appended claims.

【INDUSTRIAL APPLICABILITY】

According to the present invention, when a relay network is built for a blanket area in addition to the key network, access by the general subscriber station and the extended service subscriber station is differentiated so that the key network service provider can extend the broadcast network and the relay service provider can activate the relay business.

## 【CLAIMS】

1. A transmission system for conditionally accessing digital multimedia broadcasting (DMB) according to transmitters, the transmission system comprising:

a key center system for scrambling a transmission stream by using a control word that is generated by using first transmitter identification information, encrypting the transmission stream, and transmitting encrypted broadcast signals having the first transmitter identification information through a key network;

a relay system for receiving the encrypted broadcast signals from the key center system, inserting second transmitter identification information other than the first transmitter identification information into the encrypted broadcast signals, and transmitting the same, the second transmitter identification information being generated by the key center system from the first transmitter identification information according to a predetermined matching algorithm; and

an authentication system for receiving the matching key from the key center system, and transmitting the matching key to an extended service subscriber station that is available for a service provided by the relay system, the matching key being used to detect the first transmitter identification information from the second transmitter identification information.

2. The transmission system of claim 1, wherein the key center system comprises:

a service multiplexer for multiplexing audio, video, data, and additional information provided by a plurality of respective contents providers into transmission streams;

a first transmitter identification information generator for generating first transmitter identification information of the key center system, and generating a control word by using the generated first transmitter identification

information;

a scrambler for scrambling the multiplexed transmission streams according to a predetermined rule by using the control word so that a user without an entitlement may not receive the transmission stream;

an encryptor for encrypting the transmission stream output by the scrambler, including the first transmitter identification information and the control word into the encrypted stransmission stream, and outputting encrypted data;

a system multiplexer for multiplexing the encrypted data output by the encryptor into an ensemble transmission stream; and

a transmitter for transmitting the multiplexed signals output by the system multiplexer as encrypted broadcast signals through the key network.

3. The transmission system of claim 1 or claim 2, wherein the key center system further comprises a key table for storing a session key corresponding to the first transmitter identification information, and generates the control word by using the session key corresponding to the first transmitter identification information.

4. The transmission system of claim 3, wherein the key center system periodically modifies the first transmitter identification information and regenerates the control word by applying the modified first transmitter identification information.

5. The transmission system of claim 3, wherein the first transmitter identification information and the control word are transmitted to the relay system and the authentication system through a synchronization channel.

6. The transmission system of claim 3, wherein the control word has a different value for each transmission stream and is periodically modified

to be scrambled.

7. The transmission system of claim 3, wherein the key center system generates an entitlement control message (ECM) having the control word and transmits the ECM to a subscriber station.

8. The transmission system of claim 7, wherein the entitlement control message (ECM) is transmitted to the relay system and the authentication system through a fast information channel (FIC), and is transmitted to the extended service subscriber station from the authentication system according to a request by the extended service subscriber station.

9. The transmission system of claim 3, wherein at least one bit of the symbol that forms the first transmitter identification information is used as an error check code (ECC) of the control word.

10. The transmission system of claim 3, wherein the control word is divided into synchronization channels of a plurality of frames and is then transmitted.

11. The transmission system of claim 3, wherein the relay system comprises:

a second transmitter identification information inserter for inserting the second transmitter identification information other than the first transmitter identification information from among the encrypted broadcast signals received from the key center system;

a multiplexer/modulator for multiplexing and modulating a signal that is output by the second transmitter identification information inserter; and

a transmitter for transmitting the multiplexed and modulated signal to the subscriber station or transmitting the same to a gap filler in a blanket area through a relay link.

12. The transmission system of claim 11, wherein the relay system further comprises:

a third transmitter identification information generator for generating third gap filler transmitter identification information;

a GF multiplexer/modulator for modifying the second transmitter identification information of the encrypted broadcast signals received from the relay system into the third GF transmitter identification information, and then multiplexing and modulating the same; and

a GF transmitter for transmitting the multiplexed and modulated broadcast signals to the subscriber station.

13. The transmission system of claim 1, wherein the authentication system transmits the matching key to the extended service subscriber station through a wireless network when the extended service subscriber station has a wireless modem.

14. The transmission system of claim 1, wherein the authentication system transmits the matching key to the extended service subscriber station through a digital multimedia broadcasting (DMB) network when the extended service subscriber station has no wireless modem.

15. A transmission method for conditionally accessing digital multimedia broadcasting (DMB) according to transmitters, the transmission method comprising:

a) generating a control word by using first transmission identification information for indicating that a transmitter is a key center;

b) scrambling transmission streams including audio, video, and data provided by a plurality of contents providers by using the control word;

c) encrypting the transmission stream scrambled in b), and ensemble multiplexing the transmission stream together with the first transmission

identification information and the control word; and

d) modulating the multiplexed broadcast signal into a transmission signal, and transmitting the same through a key network.

16. The transmission method of claim 15, wherein the key center modifies the first transmitter identification information for each predetermined period to repeat the steps of a) to d).

17. The transmission method of claim 15, wherein in d), when the transmission signal is transmitted to a specific relay system, second transmitter identification information corresponding to the specific relay system is inserted into the transmission signal, wherein the second transmitter identification information is generated by the key center from the first transmitter identification information according to a predetermined matching algorithm.

18. A transmission method for conditionally accessing digital multimedia broadcasting (DMB) according to transmitters, the method comprising:

a) receiving encrypted broadcast signals from a key center, the encrypted broadcast signals including second transmitter identification information that is generated by the key center from first transmitter identification information that is the key center's identification information by using a specific matching algorithm;

b) analyzing the received broadcast signals' second transmitter identification information, and inserting the second transmitter identification information other than the first transmitter identification information into the broadcast signals transmitted to a subscriber; and

c) multiplexing/modulating the broadcast signals having the second transmitter identification information, and transmitting the broadcast signals to a subscriber station.

19. The transmission method of claim 18, further comprising:

transmitting the broadcast signals to a gap filler within the blanket area through a relay link when the subscriber station is located in a blanket area in c);

generating third transmitter identification information by the gap filler within the blanket area, and modifying the second transmitter identification information transmitted by the relay center into the third transmitter identification information; and

multiplexing/modulating the broadcast signals in which the third transmitter identification information is inserted, and transmitting the same to the subscriber station.

20. The transmission method of claim 18, wherein when the subscriber station is an extended service subscriber station that is available for a service provided by the relay center, a matching key is provided to decrypt the broadcast signals transmitted by the relay center and reproduce the same, and the matching key is used to detect the first transmitter identification information from the second transmitter identification information.

21. A system for conditionally accessing digital multimedia broadcasting (DMB) according to transmitters, the system comprising:

a transmitter identification information detector for detecting transmitter identification information from encrypted broadcast signals that are received through an antenna;

a matcher for finding transmitter identification information of a key network corresponding to transmitter identification information detected by the transmitter identification information detector, and outputting a corresponding session key;

a control word generator for generating a control word by using the

session key generated by the matcher;

a decoder for decrypting the received encrypted broadcast signals by using the control word generated by the control word generator; and

a controller for decrypting the received encrypted broadcast signals by controlling the transmitter identification information detector, the matcher, the control word generator, and the decoder according to the broadcast network to which the transmitter determined by the transmitter identification information detected by the transmitter identification information detector belongs and according to the status whether the system is registered to an extended service.

22. The system of claim 21, wherein the matcher finds transmitter identification information of the key network corresponding to the transmitter identification information detected by the transmitter identification information detector by using a matching key that is externally provided.

23. The system of claim 22, further comprising a wireless modem for externally receiving the matching key through a radio network, and transmitting the matching key to the matcher.

24. The system of claim 22, wherein the controller externally receives the matching key through the DMB network, and transmits the matching key to the matcher.

25. The system of claim 21, wherein when the controller analyzes the transmitter identification information detected by the transmitter identification information detector to determine that the encrypted broadcast signals are transmitted from the transmitter belonging to the key network, the controller controls the decoder to decrypt the encrypted broadcast signals by using the control word included in the encrypted broadcast signals.

26. The system of claim 21, wherein when the controller analyzes the transmitter identification information detected by the transmitter identification information detector to determine that the encrypted broadcast signals are transmitted from the transmitter belonging to the relay network, the controller controls the decoder to decrypt the encrypted broadcast signals by using the control word generated by the control word generator.

27. The system of any one of claims 22 to 24, wherein the matching key is exterminally received for each predetermined period.

28. A method for conditionally accessing digital multimedia broadcasting (DMB) in an extended service subscriber system, the method comprising:

a) the extended service subscriber system receiving encrypted broadcast signals from a key center or a relay center;

b) detecting transmitter identification information from a synchronization channel;

c) checking whether the detected transmitter identification information is the key center's transmitter identification information;

d) the extended service subscriber system externally receiving a matching key through the DMB network or a radio network when it is determined that the detected transmitter identification information is not the key center's transmitter identification information; and

e) decrypting the received broadcast signals by using the matching key and the detected transmitter identification information.

29. The method of claim 28, wherein e) comprises:

detecting the key center's identification information corresponding to the detected transmitter identification information by using the matching key;

detecting a session key corresponding to the detected key center's identification information;

generating a control word by using the detected session key; and

decrypting the encrypted broadcast signals by using the generated control word.

30. The method of claim 28, further comprising, in c), when it is determined that the detected transmitter identification information is the key center's transmitter identification information, the extended service subscriber system decrypting the encrypted broadcast signals by using the control word included in the encrypted broadcast signals.

31. A method for a general service subscriber to conditionally access digital multimedia broadcasting according to transmitters, the method comprising:

a) the general service subscriber system receiving encrypted broadcast signals from a key center ot a relay center;

b) detecting transmitter identification information from a synchronization channel;

c) checking whether the detected transmitter identification information is the key center's transmitter identification information; and

d) the general service subscriber system decrypting the encrypted broadcast signals by using the control word included in the encrypted broadcast signals when the detected transmitter identification information is not the key center's transmitter identification information.

32. The method of claim 31, wherein c) comprises:

increasing a value of a counter provided in the general service subscriber system when the detected transmitter identification information is not the key center's transmitter identification information;

checking whether the value of the counter corresponds to a period value established by the key center; and

resetting the value of the counter to terminate decryption on the

encrypted broadcast signals and control the access to the broadcast signals when it is determined that the value of the counter corresponds to the period value established by the key center.