InterWorking Function for Mission Critical Push to Talk Services

Chih-Cheng Tseng[1](✉), Shao-Yu Lien[2], Chuan-Xian Zhuang[1], Fang-Chang Kuo[1], and Hwang-Cheng Wang[1]

[1] National Ilan University, Yilan City, Taiwan
tsengcc@niu.edu.tw
[2] National Chung Cheng University, Chiayi, Taiwan

Abstract. Due to the continuous development of mobile communication technologies, commercialized mobile communication systems have been globally deployed. Among them, LTE-A (Long-Term Evolution-Advanced) has been adopted by several countries for the next generation PSNs (Public Safety Networks). To this end, 3GPP has also standardized Mission Critical Push To Talk (MCPTT) services in Release 13. Since the LMR (Land Mobile Radio) system has been widely adopted as the primary technology of the PSNs for a long time, it will take several years for LTE-A to replace it completely. Consequently, issues related to the interconnection of the LTE-A and LMR systems have received attention. In view of this, the interconnection of LTE-A and LMR systems has been standardized in 3GPP Release 15. A new function named IWF (InterWorking Function) was introduced to enable communications between LTE-A and LMR systems. Based on the considered system architecture, this paper first presents the implementation of IWF. Then, MCPTT group call for members between LTE-A and LMR systems is used to verify the feasibility and functionality of the implemented IWF.

Keywords: LTE-A · MCPTT · IWF · LMR

1 Introduction

1.1 Background

Land Mobile Radio (LMR) systems, including P25 (Project 25) [1] in North America and TETRA (TErrestrial Trunked RAdio) [2] in Europe, have been a legacy technology for public safety communications for decades. However, due to the advance of mobile broadband communication technologies in recent years, LTE-A (Long-Term Evolution-Advanced) system has been adopted for the next generation PSNs (Public Safety Networks) by several countries. Hence, it is estimated to take years for LTE-A system to replace the LMR system completely. Before this, it is expected that the LMR systems and the LTE-A based PSNs will coexist in the next couple of years. Consequently, interconnectivity and interoperability between the LTE-A system and the LMR system have

Y.-B. Lin et al. (Eds.): SGIoT 2021, LNICST 447, pp. 53–68, 2022.
https://doi.org/10.1007/978-3-031-20398-5_6

become critical issues. To address these issues, 3GPP has standardized MCPTT services in Release 13 [3–5]. Furthermore, 3GPP formulated a standard for the interconnection between the MC (Mission Critical) system and the LMR system. It introduced a new function named IWF (InterWroking Function) in Release 15 [6] to specify the support for the interworking between the MC system and the LMR system under the requirements defined in [5] and [7]. In [6], the term *interworking* is defined as a means of communication between the MC system and the LMR system whereby MC users obtaining service from an MC system can communicate with LMR users obtaining service from one or more LMR systems.

1.2 Motivation

Considering that MC systems will coexist with the LMR systems for a period of time, the interconnection capability between devices in MC systems and LMR systems is necessary. There are platforms on the market that enable LTE-A devices and LMR devices to connect to each other [8, 9]. However, the cost of these existing platforms is not friendly. Therefore, this paper focuses on designing and implementing a cost-effective prototype platform of the IWF.

1.3 Goal and Contributions

Among the procedures specified in [6], the following are implemented in the IWF:

- Affiliation: Allow LMR users to join a selected group via IWF.
- De-affiliation: Allow LMR users to leave the selected group via IWF.
- Group call: Allow LMR users to make group calls with other members in the same group via IWF and vice versa.
- Floor control: Allow LMR users to request for the floor to make a group call.

2 The Design and Implementation of the IWF Prototype Platform

2.1 System Architecture

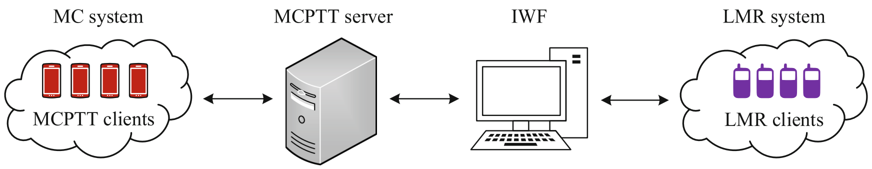

Fig. 1. System architecture

The design of the presented IWF is based on the considered system architecture (see Fig. 1). In this architecture, users in the MC system are identified by MC IDs. After authorization, they obtain MC service(s) and are regarded as MC users. Besides, users in the LMR system are regarded as LMR users. The main components of the architecture are the follows:

MC System: The MC system is defined as the collection of applications, services, and enabling capabilities required to provide a single MC service or multiple MC services to one or more MC organizations [10].

MCPTT Client: The MCPTT client is an App installed on a smartphone or pad. With the help of the installed App, the smartphone or pad provides the MCPTT services such as making group calls with other members in the same group with the help of the MCPTT server and IWF.

MCPTT Server: The MCPTT server is installed in a linux-based OS (Operating System) and is responsible for providing MCPTT services to the authenticated clients (MCPTT clients and IWF).

IWF: IN [6], IWF is defined as an entity that "*Adapts LMR systems to MC systems via the IWF interface and supports interworking between LMR systems and MC systems.*" Besides, IWF is required to support necessary protocol translation and identity mapping between the MC systems and the LMR systems. Thus, IWF can be regarded as the representative of LMR clients in the MC system. The presented IWF prototype platform is implemented in Java and is operated in a linux-based OS.

LMR System: The LMR system is the collection of applications, services, and enabling capabilities for providing LMR service of group and private communications [6].

LMR Client: The LMR client is the radio operated by an LMR user and is capable of using the MCPTT services such as making group calls with other members in the same group in the MC system with the help of the MCPTT server and IWF.

2.2 Related Protocols

The protocols of IWF can be divided into control-plane and user-plane protocols. Control plane-related protocols are based on TCP (Transmission Control Protocol) and include SIP (Session Initiation Protocol), SDP (Session Description Protocol), and HTTP (Hypertext Transfer Protocol). User plane-related protocols are based on UDP (User Datagram Protocol) and include RTP and RTCP.

SIP: SIP [11] is an application layer protocol based on TCP or UDP. SIP provides a variety of request methods (see Table 1) and response codes (see Table 2), which make it suitable for establishing, modifying, and terminating media sessions.

SDP: SDP [12] is used to negotiate the establishment of a multimedia data traffic channel between caller and callee. During the three-way handshake process of the SIP INVITE request, SDP is used to exchange the media parameters between the two endpoints.

HTTP: HTTP [13] is an application layer protocol. HTTP functions as a request-response protocol in the client-server model. In the considered system architecture, HTTP is used to get user profile and group information, such as the list of all groups in the MCPTT server.

Table 1. SIP request methods

Method	Description
REGISTER	Register the user's URI
INVITE	Establish session
ACK	Confirm that an entity has received a final response to an INVITE request
BYE	Release session
CANCEL	Cancel any pending request
UPDATE	Modify the information of a session
REFER	Ask the recipient to issue a request for the purpose of call transfer
PRACK	Provisional acknowledgment
SUBSCRIBE	Initiate a subscription for notification of events from a notifier
NOTIFY	Inform a subscriber of notifications of a new event
PUBLISH	Publish an event to a notification server
MESSAGE	Deliver a text message
INFO	Send mid-session information
OPTIONS	Query the capabilities of an endpoint

Table 2. SIP response codes

Result	Description
1xx	Provisional response to request indicating the request is valid and is being processed
2xx	Successful completion of the request
3xx	Call redirection is needed for the completion of the request
4xx	Client error: The request cannot be completed
5xx	Server error: The server fails to fulfill an apparently valid request
6xx	Global error: The request cannot be fulfilled at any server

RTCP: RTCP [14] is a UDP-based application layer protocol. The primary function of RTCP is to provide feedback on the QoS (Quality of Service) in media distribution by periodically sending statistical information such as transmitted octet and packet counts. Moreover, in 3GPP TS24.380, RTCP is adopted to implement floor control.

RTP: RTP [14] is a UDP-based application layer protocol designed exclusively for end-to-end and real-time transfer of streaming media.

3 Group Configuration Procedures

To enable LMR clients to communicate with MCPTT clients, as the representative of the LMR clients, IWF is required to affiliate to the same group as the MCPTT clients. The procedures for IWF to affiliate and de-affiliate to a group are presented below. Based on the procedures, IWF exchanges all the required messages with the MCPTT server. In this way, we ensure that all the group-related messages can be validated by the MCPTT server.

3.1 Requesting the List of Existing Groups

Before proceeding with the affiliation procedures, IWF needs to know the existing groups in the MCPTT server. To this end, the request to obtain the latest group list is embedded in the command field of the HTTP GET request. Details of this procedure are illustrated in Fig. 2 and described below.

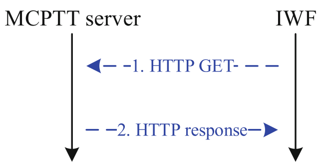

Fig. 2. Procedures to request for the list of existing groups

Step 1: To request the list of all groups that currently exist in the MCPTT server, IWF sends an HTTP GET request to the MCPTT server.

Step 2: After parsing the contents in the command field of the received HTTP GET request and verifying it as requesting for the list of existing groups, the MCPTT server replies with an HTTP response in which the latest list of all existing groups in the MCPTT server is included.

3.2 Requesting the List of Affiliated Groups

To know the groups that have been affiliated, IWF uses a procedure similar to that for requesting the list of existing groups to exchange messages with the MCPTT server. The request to obtain the list of affiliated groups is embedded in the command field of the HTTP GET request. Details of this procedure are described below.

Step 1: To request the list of groups that have been affiliated, IWF sends an HTTP GET request to the MCPTT server.

Step 2: After parsing the contents in the command field of the received HTTP GET request and verifying it as requesting for the list of affiliated groups, the MCPTT server replies with an HTTP response in which the list of groups that have been affiliated is included.

3.3 Affiliation

To affiliate to a group, IWF first selects a group that has not been affiliated. After that, IWF proceeds to execute the affiliation procedure as depicted in Fig. 3 to affiliate to the selected group. Details of this procedure are described below.

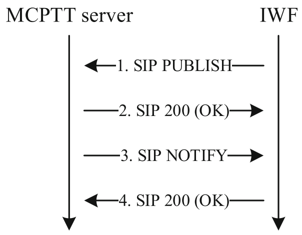

Fig. 3. Affiliation/De-affiliation procedure [3, 6]

Step 1: IWF sends a SIP PUBLISH request to the MCPTT server in which the required information, such as the name of the group to be affiliated, is included.

Step 2: MCPTT server verifies if the received SIP PUBLISH request is sent by an authorized user of IWF. If not, based on the problem found, a corresponding SIP 4xx response is replied and the procedure ends. Otherwise, MCPTT server replies with a SIP 200 (OK) response and goes to Step 3.

Step 3: MCPTT server processes the information carried in SIP PUBLISH request and sends a SIP NOTIFY request to the IWF as the notification of the affiliation result. The possible status code of affiliation is 1, 3, 4, or 6, as shown in Table 3.

Step 4: IWF replies with a SIP 200 (OK) response after correctly receiving the SIP NOTIFY request.

Note that to make a group call, IWF is required to affiliate to that group first.

Table 3. Result of affiliation/de-affiliation

Status	Description
1	The result of affiliation is successful
2	The result of de-affiliation is successful
3	The number of group members exceeds the upper limit
4	The selected group has been affiliated before
5	The selected group has not been affiliated yet
6	The selected group does not exist
7	The number of group members cannot be less than two

3.4 De-affiliation

The administrator of IWF may want to de-affiliate a group from the list of affiliated groups. In this case, the IWF executes the same procedure as it does for affiliation in Fig. 3. Details of this procedure are described below.

Step 1: IWF sends a SIP PUBLISH request to the MCPTT server in which the required information, such as the name of the group that wants to be de-affiliated, is included.

Step 2: MCPTT server verifies if the received SIP PUBLISH request is sent by an authorized user of IWF. If not, based on the problem found, a corresponding SIP 4xx response is replied and the procedure ends. Otherwise, the MCPTT server replies with a SIP 200 (OK) response and goes to Step 3.

Step 3: MCPTT server processes the information carried in SIP PUBLISH request and sends a SIP NOTIFY request to the IWF as the notification of the de-affiliation result. The possible status code of de-affiliation is 2, 5, 6, or 7, as shown in Table 3.

Step 4: IWF replies with a SIP 200 (OK) response after correctly receiving the SIP NOTIFY request.

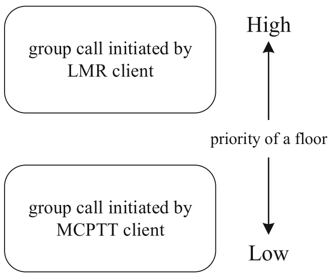

Fig. 4. Priority of a floor in the system

4 Floor Control

The members in a group can be classified as MCPTT clients and LMR clients. Consider the scenario in which an LMR client and an MCPTT client want to initiate a group call simultaneously and the LMR client successfully obtains the wireless channel to send voice messages. On receiving the voice messages, IWF sends a Floor Request message to the MCPTT server to request the floor for the LMR client. Similarly, the MCPTT client also sends a Floor Request message to the MCPTT server. Since the LMR client is operated in the half-duplex mode, it cannot transmit and receive messages simultaneously. If the MCPTT server grants the floor to the MCPTT client, there is no way to notify the LMR client that is currently in transmitting mode about this. Hence, the LMR client would not stop sending voice messages. Besides, all the voice messages from the LMR client will not be forwarded to the MCPTT clients. Although the floor is granted to the MCPTT client, IWF cannot forward all the voice messages from the

MCPTT client to the LMR client that is currently in transmitting mode. Therefore, when initiating a group call, the priority of the floor requested by the LMR client is higher than that by the MCPTT client of the same group to avoid the above problem The priority of a floor in the implemented system is shown in Fig. 4.

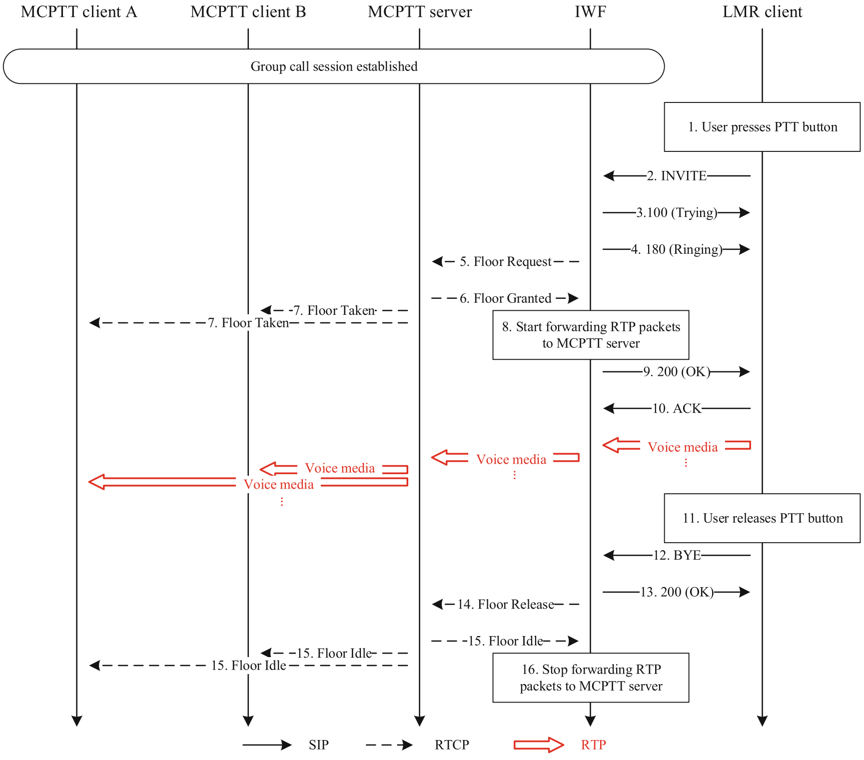

Fig. 5. LMR user initiates group call [6, 15]

5 Procedures for Initiating Group Call

5.1 LMR User Initiates Group Call

When an LMR user wants to make a group call, the following procedure will be performed (see Fig. 5).

Step 1: LMR user presses the PTT (Push To Talk) button to make a group call.

Step 2: After receiving the event that the PTT button is pressed, the LMR client sends a SIP INVITE request to the IWF.

Step 3: After successfully receiving the SIP INVITE request, IWF replies with a SIP 100 (Trying) response to the LMR client.

Step 4: IWF replies with a SIP 180 (Ringing) response notifying the LMR client that the media parameters carried in the SIP INVITE request are being processed.

Step 5: IWF sends a Floor Request message to the MCPTT server.

Step 6: After receiving the Floor Request, based on the priority of the request (see Fig. 4), the MCPTT server responds with a Floor Granted message to the IWF.

Step 7: The MCPTT server sends a Floor Taken message to the other members in the group call to notify them that IWF obtains the floor.

Step 8: After receiving the Floor Granted message, IWF enables the function of forwarding RTP packets to forward RTP packets from the LMR client to the MCPTT server.

Step 9: IWF includes its media parameters in a SIP 200 (OK) and sends the SIP 200 (OK) to the LMR client.

Step 10: After receiving the SIP 200 (OK) response, the LMR client analyzes and stores the media parameters carried in the SIP 200 (OK) response and replies with a SIP ACK to IWF.

After Step 10, the RTP packets generated by the LMR client are forwarded hop-by-hop to the other two group members, MCPTT clients A and B, in the MC system.

Step 11: LMR user releases the PTT button to terminate this group call.

Step 12: After receiving the event that the PTT button is released, the LMR client sends a SIP BYE request to the IWF.

Step 13: After receiving the SIP BYE request, IWF first replies with a SIP 200 (OK) to the LMR client. Then, IWF deletes the connection to the LMR client.

Step 14: IWF sends a Floor Release message to the MCPTT server to release the floor.

Step 15: After receiving the Floor Release message, the MCPTT server sends a Floor Idle message to all group members in this group call.

Step 16: After receiving the Floor Idle message, IWF disables the function of forwarding RTP packets to stop sending RTP packets from the LMR client to the MCPTT server.

5.2 MC User Initiates Group Call

When the MC user of MCPTT client A wants to make a group call, the following procedure will be performed (see).

Step 1: MC user presses the PTT button to make a group call.

Step 2: After receiving the event that the PTT button is pressed, MCPTT client A sends a Floor Request to the MCPTT server.

Step 3: Since only the Floor Request from MCPTT client A is received, based on the priority of the floor (see), the MCPTT server responds with a Floor Granted message to the MCPTT client A.

Step 4: The MCPTT server sends a Floor Taken message to other members participating in this group call to notify that MCPTT client A obtains the floor.

Step 5: After receiving the Floor Taken message, IWF sends a SIP INVITE request to the LMR client.

Step 6: After receiving the SIP INVITE request, the LMR client replies with a SIP 100 (Trying) response.

Step 7: LMR client continues to reply with a SIP 183 (Session Progress) response notifying IWF that the media parameters in the SIP INVITE request are being processed.

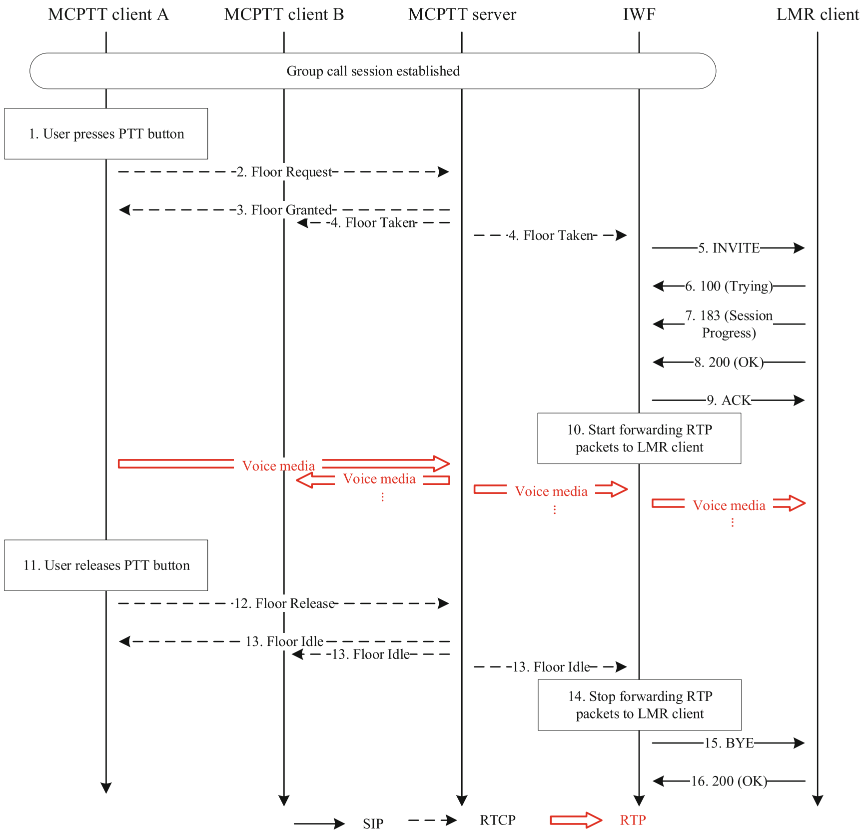

Fig. 6. MC user initiates group call [6, 15]

Step 8: LMR client includes its media parameters in a SIP 200 (OK) and replies with the SIP 200 (OK) to the IWF.

Step 9: After receiving the SIP 200 (OK) response, IWF analyzes and stores the media parameters carried in the SIP 200 (OK) response and replies with a SIP ACK to the LMR client.

Step 10: IWF enables the function of forwarding RTP packets and sends the RTP packets from the MCPTT server to the LMR client.

Step 11: MC user releases the PTT button to terminate this group call.

Step 12: After receiving the event that the PTT button is released, MCPTT client A forwards a Floor Release message to the MCPTT server.

Step 13: After receiving the Floor Release message, the MCPTT server sends a Floor Idle message to all group members participating in this group call.

Step 14: After receiving the Floor Idle message, IWF disables the function of forwarding RTP packets and stops sending RTP packets from the MCPTT server to the LMR client.

Step 15: IWF sends a SIP BYE request to the LMR client.

Step 16: After receiving the SIP BYE request, the LMR client replies with a SIP 200 (OK) and then deletes the connection with IWF.

6 Verification of the Implemented Procedures

Wireshark [16] was used to capture the exchanged packets while performing each of the procedures mentioned above for the verification of the procedures in the following use cases.

6.1 Group Configuration

Requesting the List of Existing Groups. The detailed description of the use case of requesting the list of existing groups and the corresponding captured packets are shown in Table 4 and Fig. 7, respectively. By comparing Fig. 2 with Fig. 7, we see that all the packets involved in the procedure for requesting the list of existing groups are correctly exchanged. Hence, the procedure for requesting the list of existing groups is verified.

Table 4. Use case of requesting the list of existing groups

Requesting the list of existing groups	
Description	The IWF requests the list of existing groups in the MCPTT server
Participants	MCPTT server and IWF
Post-conditions	The IWF obtains the list of existing groups
Note: IP address of the MCPTT server is 140.123.102.114 and IP address of IWF is 120.101.9.174	

Source	Destination	Protocol	Length	Info
120.101.9.174	140.123.102.114	HTTP	236	GET /restcomm/?cmd=GetAllGroupList HTTP/1.1
140.123.102.114	120.101.9.174	HTTP	60	HTTP/1.1 200 OK (text/plain)

Fig. 7. Captured packets for requesting the list of existing groups

Table 5. Use case of requesting the list of affiliated groups

Requesting the list of affiliated groups	
Description	The IWF requests the list of affiliated groups from the MCPTT server
Participants	MCPTT server and IWF
Post-conditions	The IWF obtains the list of affiliated groups
Note: IP addresses of MCPTT server and IWF are 140.123.102.114 and 120.101.9.174, respectively	

Requesting the List of Affiliated Groups. The detailed description of the use case of requesting the list of affiliated groups and the corresponding captured packets are shown in Table 5 and Fig. 8, respectively. Comparison of Fig. 2 and Fig. 8 reveals that all the required packets concerning the procedure for requesting the list of affiliated groups are correctly exchanged. Hence, the procedure for requesting the list of affiliated groups is verified.

Source	Destination	Protocol	Length	Info
120.101.9.174	140.123.102.114	HTTP	352	GET /restcomm/?cmd=GetData&Parm=140.123.102.114:15060/xcap-root
140.123.102.114	120.101.9.174	HTTP/XML	60	HTTP/1.1 200 OK

Fig. 8. Captured packets for requesting the list of affiliated groups

Table 6. Use case of affiliation

Affiliation	
Description	According to the list of existing groups, user selects one to affiliate. After the group is selected, IWF executes the affiliation procedure
Participants	MCPTT server and IWF
Post-conditions	According to the result included in the SIP NOTIFY request (see **Table 3**), IWF knows if it has successfully been affiliated to the selected group

<table>
<tr><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr>
<tr><td>120.101.9.174</td><td>140.123.102.114</td><td>SIP/XML</td><td>1506</td><td>Request: PUBLISH sip:EMCard31@140.123.102.114 | (application/vnd.3gpp.mcptt-info+xml)</td></tr>
<tr><td>140.123.102.114</td><td>120.101.9.174</td><td>SIP</td><td>344</td><td>Status: 200 OK |</td></tr>
<tr><td>140.123.102.114</td><td>120.101.9.174</td><td>SIP/XML</td><td>969</td><td>Request: NOTIFY sip:EMCard31@120.101.9.174:1434;transport=tcp |</td></tr>
<tr><td>120.101.9.174</td><td>140.123.102.114</td><td>SIP</td><td>441</td><td>Status: 200 OK |</td></tr>
</table>

Fig. 9. Captured packets for affiliating to the selected group

Affiliation. The detailed description of the use case of affiliation and the corresponding captured packets are shown in Table 6 and Fig. 9, respectively. From Fig. 3 and Fig. 9, it is clear that all the packets required by the procedure for affiliation are correctly exchanged. Hence, the procedure for affiliation is verified.

Table 7. Use case of de-affiliation

De-affiliation	
Description	According to the list of affiliated groups, user selects one to de-affiliate. After the group is selected, IWF executes the de-affiliation procedure
Participants	MCPTT server and IWF
Post-conditions	According to the result included in the SIP NOTIFY request (see Table 3), IWF knows if the selected group has successfully been de-affiliated

<table>
<tr><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr>
<tr><td>120.101.9.174</td><td>140.123.102.114</td><td>SIP/XML</td><td>1500</td><td>Request: PUBLISH sip:EMCard31@140.123.102.114 | (application/vnd.3gpp.mcptt-info+xml)</td></tr>
<tr><td>140.123.102.114</td><td>120.101.9.174</td><td>SIP</td><td>344</td><td>Status: 200 OK |</td></tr>
<tr><td>140.123.102.114</td><td>120.101.9.174</td><td>SIP/XML</td><td>972</td><td>Request: NOTIFY sip:EMCard31@120.101.9.174:1434;transport=tcp |</td></tr>
<tr><td>120.101.9.174</td><td>140.123.102.114</td><td>SIP</td><td>441</td><td>Status: 200 OK |</td></tr>
</table>

Fig. 10. Captured packets for de-affiliating the selected group

De-affiliation. The detailed description of the use case of de-affiliation and the corresponding captured packets are shown in Table 7 and Fig. 10, respectively. Comparion of Fig. 3 and Fig. 10 shows that all the required packets in the procedure for de-affiliation are correctly exchanged. Hence, the procedure for de-affiliation is verified.

6.2 LMR User Initiating Group Call

The detailed description of the use case of an LMR user initiating a group call is listed in Table 8, while the corresponding captured packets are shown in Fig. 11, Fig. 12, Fig. 13, and Fig. 14, respectively. Results in Fig. 11, Fig. 12, Fig. 13, and Fig. 14 indicate that all the required packets (see Fig. 5) in the procedure for an LMR user to initiate a group call are correctly exchanged. Hence, the the correctness of procedure is verified.

Table 8. Use case of LMR user initiating group call

LMR user initiates group call	
Description	The LMR user wants to initiate a group call
Participants	MCPTT server and IWF
Post-conditions	The RTP packets of the LMR client are forwarded by the IWF and the MCPTT server to the other group members in this group call
Note: Note: IP addresses of MCPTT server and IWF are 140.123.102.114 and 120.101.9.174, respectively. Private IP addresses of LMR client and IWF are 192.168.28.151 and 192.168.28.1, respectively	

<table>
<tr><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr>
<tr><td>192.168.28.151</td><td>192.168.28.1</td><td>SIP/SDP</td><td>889</td><td>Request: INVITE sip:402@192.168.28.1 |</td></tr>
<tr><td>192.168.28.1</td><td>192.168.28.151</td><td>SIP</td><td>416</td><td>Status: 100 Trying |</td></tr>
<tr><td>192.168.28.1</td><td>192.168.28.151</td><td>SIP</td><td>416</td><td>Status: 180 Ringing |</td></tr>
<tr><td>192.168.28.1</td><td>192.168.28.151</td><td>SIP/SDP</td><td>774</td><td>Status: 200 OK |</td></tr>
<tr><td>192.168.28.151</td><td>192.168.28.1</td><td>SIP</td><td>388</td><td>Request: ACK sip:407@192.168.28.1 |</td></tr>
</table>

Fig. 11. Captured packets for LMR client to establish a session to IWF

<table>
<tr><th>Source</th><th>Destination</th><th>Protocol</th><th>Length</th><th>Info</th></tr>
<tr><td>120.101.9.174</td><td>140.123.102.114</td><td>RTCP</td><td>94</td><td>(MCPT) Floor Request[Malformed Packet]</td></tr>
<tr><td>140.123.102.114</td><td>120.101.9.174</td><td>RTCP</td><td>74</td><td>(MCPT) Floor Granted[Malformed Packet]</td></tr>
</table>

Fig. 12. Captured packets for IWF to obtain the floor

Source	Destination	Protocol	Length	Info
120.101.9.174	140.123.102.114	RTCP	90	(MCPT) Floor Release[Malformed Packet]
140.123.102.114	120.101.9.174	RTCP	62	(MCPT) Floor Idle[Malformed Packet]

Fig. 13. Captured packets for IWF to release the floor

Source	Destination	Protocol	Length	Info
192.168.28.151	192.168.28.1	SIP	389	Request: BYE sip:402@192.168.28.1 |
192.168.28.1	192.168.28.151	SIP	365	Status: 200 OK |

Fig. 14. Captured packets for LMR client to release a session to IWF

6.3 MC User Initiating Group Call

The detailed description of the use case of an MC user initiating a group call is listed in Table 9, while the corresponding captured packets are shown in Fig. 15, Fig. 16, Fig. 17, and Fig. 18, respectively. These figures show that all the required packets, as depicted in Fig. 6 in the procedure for an MC user to initiate a group call, are correctly exchanged. Hence, the correctness of the procedure is verified.

Table 9. Use case of MC user initiating group call

LMR user initiates group call	
Description	The MC user wants to initiate a group call
Participants	MCPTT server and IWF
Post-conditions	The RTP packets of MCPTT client are forwarded by the MCPTT server and the IWF to other group members in this group call
Note: Note: IP addresses of MCPTT server and IWF are 140.123.102.114 and 120.101.9.174, respectively. Private IP addresses of LMR client and IWF are 192.168.28.151 and 192.168.28.1, respectively	

Source	Destination	Protocol	Length	Info
140.123.102.114	120.101.9.174	RTCP	106	(MCPT) Floor Taken[Malformed Packet]

Fig. 15. Captured packet for IWF to be informed about the floor has been taken

Source	Destination	Protocol	Length	Info
192.168.28.1	192.168.28.151	SIP/SDP	888	Request: INVITE sip:407@192.168.28.151 |
192.168.28.151	192.168.28.1	SIP	415	Status: 100 Trying |
192.168.28.151	192.168.28.1	SIP	416	Status: 180 Ringing |
192.168.28.151	192.168.28.1	SIP/SDP	787	Status: 200 OK |
192.168.28.1	192.168.28.151	SIP	372	Request: ACK sip:407@192.168.28.151 |

Fig. 16. Captured packets for IWF to establish a session to the LMR client

Source	Destination	Protocol	Length	Info
140.123.102.114	120.101.9.174	RTCP	62	(MCPT) Floor Idle[Malformed Packet]

Fig. 17. Captured packet for IWF to be informed about the floor is idle

Source	Destination	Protocol	Length	Info
192.168.28.1	192.168.28.151	SIP	372	Request: BYE sip:407@192.168.28.151 |
192.168.28.151	192.168.28.1	SIP	361	Status: 200 OK |

Fig. 18. Captured packets for IWF to release the session to LMR client

7 Conclusion

To achieve the interworking between MC systems and LMR systems, IWF was standardized by the 3GPP. Based on the standardized IWF and the considered system architecture, a simplified IWF prototype platform has been implemented based on the six considered use cases: Requesting The List of Existing Groups, Requesting The List of Affiliated Groups, Affiliation, De-affiliation, LMR User Initiating Group Call, and MC User Initiating Group Call. Procedures for the six considered use cases have been developed. We used Wireshark to capture the packets exchanged to verify the operability and applicability of the developed procedures. Carefully comparing the developed procedures and the captured packets confirmed the operability and applicability of the six use cases. In addition to further increasing the MCPTT use cases for the implemented IWF prototype platform, we intend to support more MC services (e.g., MCData [7] and MCVideo [17]) in the future.

Acknowledgment. This work was supported in part by the Ministry of Science and Technology, Taiwan, R. O. C., under grant number MOST 109–2221-E-197–028-MY3.

References

1. APCO: "Project 25 Push-to-X" website, https://www.apcointl.org/spectrum-management/spectrum-management-resources/interoperability/p25/. Last accessed 30 August 2021
2. ETSI: "TErrestrial Trunked RAdio" website, https://www.etsi.org/technologies/tetra. Last accessed 30 August 2021
3. 3GPP: Functional architecture and information flows to support Mission Critical Push to Talk (MCPTT), TS 23.379 (July 2020)
4. 3GPP: Mission Critical Push to Talk (MCPTT) call control (Release 16), TS 24.379 (June 2021)
5. 3GPP: Mission Critical Push to Talk over LTE requirements (Release 16), TS 22.179 (March 2019)
6. 3GPP: Mission Critical Communication Interworking with Land Mobile Radio Systems (Release 16), TS 23.283 (Sept 2020)
7. 3GPP: Mission Critical Data over LTE (Release 14), TS 22.282 (March 2017)
8. SAMSUNG: "Solving Critical Communication Challenges with Mission Critical Push-to-X" website, https://images.samsung.com/is/content/samsung/assets/global/business/networks/insights/white-paper/samsung-mcptx/Samsung_MCPTX_SolutionBrief_FINAL_r1.pdf. Last accessed 22 August 2021

9. Catalyst: “Interworking - Catalyst Communication Technologies” website, https://www.catcomtec.com/technology/lmr-lte-interworking/. Last accessed 22 August 2021
10. 3GPP: Common Functional Architecture to Support Mission Critical Services (Release 17), TS 23.280 (June 2021)
11. Rosenberg, J. et al.: SIP: Session Initiation Protocol, RFC 3261 (June 2002)
12. Handley, M., Mark, V.J., Perkins, C.: SDP: Session Description Protocol, RFC 4566 (July 2006)
13. Fielding, R., et al.: Hypertext Transfer Protocol -- HTTP/1.1, RFC 2616 (June 1999)
14. Schulzrinne, H., Casner, S., Frederick, R., Jacobson, V.: RTP: A Transport Protocol for Real-Time Applications, RFC 3550 (July 2003)
15. 3GPP: Technical Specification Group Core Network and Terminals Mission Critical Push To Talk (MCPTT) media plane control, TS 24.380 (Dec. 2019)
16. Wireshark: https://www.wireshark.org/. Last accessed 22 August 2021
17. 3GPP: Mission Critical Video over LTE (Release 14), TS 22.281 (March 2017)