IEEE P802.16p REV3 AWD

Part 16: Air Interface for Broadband Wireless Access Systems —

Enhancements to Support Machine-to-Machine Applications

~~Sponsor~~

~~**LAN/MAN Standards Committee**~~
~~of the~~
~~**IEEE Computer Society**~~

~~and the~~

~~**IEEE Microwave Theory and Techniques Society**~~

Introduction

This introduction is not part of IEEE Std 802.16p, IEEE Standard for Local and metropolitan area networks—Part 16: Air Interface for Broadband Wireless Access Systems - Amendment: Air Interface for Broadband Wireless Access Systems – Enhancements to Support Machine-to-Machine Applications.

This amendment specifies support for Machine-to-Machine Applications. As of the publication date, the current applicable version of IEEE Std 802.16 is IEEE Std 802.16-2009, as amended by IEEE 802.16j-2009, IEEE 802.16h-2010, and IEEE 802.16m-2011.

Notice to users

Laws and regulations

~~Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.~~

Copyrights

~~This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.~~

Updating of IEEE documents

~~Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.~~

~~For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at http://standards.ieee.org.~~

Errata

~~Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.~~

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

~~***[The following notice shall appear when the IEEE receives assurance from a known patent holder or patent applicant prior to the time of publication that a license will be made available to all applicants either without compensation or under reasonable rates, terms, and conditions that are demonstrably free of any unfair discrimination.]***~~

~~Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. A patent holder or patent applicant has filed a statement of assurance that it will grant licenses under these rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses. Other Essential Patent Claims may exist for which a statement of assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions are reasonable or non-discriminatory. Further information may be obtained from the IEEE Standards Association.~~

~~***[If the IEEE has not received letters of assurance prior to the time of publication, the following notice shall appear:]***~~

~~Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.~~

Participants

This document was developend by the IEEE 802.16 Working Group on Broadband Wireless Access, which develops the WirelessMAN® Standard for Wireless Metropolitan Area Networks.

Roger B. Marks, *Chair*
Rakesh Taori, *Vice-Chair*
Erik Colban, *Secretary*
Scott Migaldi, *Treasurer*

The following members of the IEEE 802.16 Working Group on Broadband Wireless Access participated in the Working Group Letter Ballot in which the draft of this standard was prepared and finalized for IEEE Ballot:

~~Yan Xiu Zheng~~ ~~Lei Zhou~~ ~~Jing Zhu~~
~~Hua Zhou~~ ~~Chenxi Zhu~~ ~~Peiying Zhu~~

Primary development was carried out by the Working Group's Task Group p.

TGp Leadership Team:

Ron Murias, Chair
TBD, Vice Chair
TBD, Secretary
Hyunjeong Kang, Chief Editor, 802.16p
Jin Lee, Editor, System Requirements Document
HanGyu Cho, Editor, M2M Technical Report

The following members of the [individual/entity] balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

When the IEEE-SA Standards Board approved this standard on XX Month 2008, it had the following membership:

Robert M. Grow, *Chair*
Thomas Prevost, *Vice Chair*
Steve M. Mills, *Past Chair*
Judith Gorman, *Secretary*

Victor Berman	Jim Hughes	Chuck Powers
Richard DeBlasio	Richard H. Hulett	Narayanan Ramachandran
Andy Drozd	Young Kyun Kim	Jon Walter Rosdahl
Mark Epstein	Joseph L. Koepfinger*	Robby Robson
Alexander Gelman	John Kulick	Anne-Marie Sahazizia
William R. Goldbach	David J. Law	Malcolm V. Thaden
Arnold M. Greenspan	Glenn Parsons	Howard L. Wolfman
Kenneth S. Hanus	Ronald C. Petersen	Don Wright

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Michael H. Kelly, *NIST Representative*

Your name here
IEEE Standards Program Manager, Document Development

Your name here
IEEE Standards Program Manager, Technical Program Development

Contents

List of Figures

List of Tables

Amendment Working Document (AWD) to IEEE Standard for

Local and metropolitan area networks

Part 16: Air Interface for Broadband Wireless Access Systems —

Enhancements to Support Machine-to-Machine Applications

NOTE-The editing instructions contained in this amendment define how to merge the material contained herein into the existing base standard IEEE Std 802.16-2009 as amended by IEEE Std 802.16j, IEEE Std 802.16h, and IEEE 802.16m. The editing instructions are shown in ***bold italic***. Four editing instructions are used: ***change***, ***delete***, ***insert***, and ***replace***. ***Change*** is used to make small corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using strike through (to remove old material) and underscore (to add new material). ***Delete*** removes existing material. ***Insert*** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make large changes in existing text, subclauses, tables, or figures by removing existing material and replacing it with new material. Editorial notes will not be carried over into future editions because the changes will be incorporated into the base standard.

1. Overview

1.1 Scope

1.2 Purpose

3. Definitions

Add the following definitions:

3.224 Machine-to-Machine (M2M) communication: Information exchange between user devices through a Base Station, or between a device and a server in the core network through a Base Station that may be carried out without any human interaction.

3.225 M2M ASN: An Access Service Network that supports M2M service

3.226 M2M device: An MS that is capable of providing M2M communication

3.227 M2M Server: An entity that communicates with M2M devices. The M2M server runs M2M applications and provides M2M specific services for one or more M2M devices.

3.228 M2M feature: A unique characteristic of an M2M application that is supported by the M2M ASN. One or more features may be needed to support an application.

3.229 M2M group: A group of M2M devices that share one or more features in common

6. MAC common part sublayer

6.3 Data/Control plane

6.3.1 Addressing and connections

Insert the following texts at the end of subclause 6.3.1

A 15-bit M2M group ID (MGID) uniquely identifies an M2M group in the domain of the network entity that assigns MGID.

An MGID is assigned to a service flow of an M2M device by a network entity after initial network entry through DSA procedure and released during an explicit network exit (e.g., power down location update). The assigned MGID shall be retained by an M2M device even in idle state unless the M2M device exits from the network. The MGID can be re-assigned during normal mode and idle mode. During normal mode, the MGID may be changed by DSC procedure. Reassignment procedure during idle mode is TBD.

6.3.2.3 MAC management messages

6.3.2.3.5 RNG-REQ (ranging request) message

Change the paragraph as follows:

The following TLV parameter shall be included in the RNG-REQ message when the MS is attempting to perform reentry, HO, or location update:

Ranging Purpose Indication

The presence of this item in the message indicates the following MS action:

If Bit 0 is set to 1, in combination with a serving BSID, it indicates that the MS is currently attempting to HO or reentry; or, in combination with a Paging Controller ID, indicates that the MS is attempting network reentry from idle mode to the BS.

If Bit 1 is set to 1, it indicates that the MS is initiating the idle mode location update process.

Bit 2: Seamless HO indication. When this bit is set to 1 in combination with other included information elements, it indicates the MS is initiating ranging as part of seamless HO procedure.

Bit 3: Ranging Request for Emergency Call Setup. When this bit is set to 1, it indicates MS action of Emergency Call Process.

Bit 4: MBS update. When this bit is set to 1, the MS is currently attempting to perform location update due to a need to update service flow management encodings for MBS flows.

Bit 5: Abnormal Power Down Indication. When this bit is set to 1, MS indicates that an abnormal or involuntary power down occurs.

Bits 6~~5~~–7: Reserved

Add the following texts at the end of the subclause 6.3.2.3.5 as indicated

The following TLV parameters may be included in an RNG-REQ message when the Matrix A or Matrix B is supported by fixed M2M device:

MIMO Feedback information

This TLV includes the 1 bit Matrix indicator indicating the preferred STC/MIMO matrix and 4-bit DL Effective CINR as defined in Table 520.

The following parameter indicates the number of ranging retries during the current ranging process performed by an M2M device. This TLV may be included by M2M devices when performing initial ranging for network entry or re-entry, periodic ranging, or HO ranging:

Ranging Retries

After the station entered the Localized Idle Mode (i.e., Localized_Idle_Mode_Accepted flag is set to 1 in DREG-REQ/CMD), when the station sends a RNG-REQ message for reentry or location update to a BS, the BS shall not include Paging Controller ID TLV (see 11.1.8.2) in this message.

6.3.2.3.6 RNG-RSP (ranging response) message

Add the following texts at the end of the subclause 6.3.2.3.6 as indicated

After the station entered the Localized Idle Mode (i.e., Localized_Idle_Mode_Accepted flag is set to 1 in DREG-REQ/CMD), when the BS sends a RNG-RSP message for reentry or location update to a station, following Paging Information TLV is included and Paging Controller ID TLV (see 11.1.8.2) is not included in this message.

Paging Information TLV

Bits 0-15: PAGING_CYCLE - cycle in which the paging message is transmitted within the paging group.

Bits 16-31:PAGING_OFFSET - determines the frame within the cycle from which the paging interval starts. Shall be smaller than PAGING_CYCLE value.

Bits 32-39: Paging Interval Length - Max duration in frames of Paging listening interval. Used in calculation of Paging listening interval; value shall be between 1 and 5 frames (default=2).

6.3.2.3.9 Privacy key management (PKM) messages (PKM-REQ/PKM-RSP)

Change the contents of Table 66 as follows

Table 66—PKM message codes

Code	PKM message type	MAC management message name
...	...	...
33	MIH Comeback Response	PKM-RSP
34	PKMv2 AK Transfer	PKM-RSP
35	PKMv2 AK Transfer Ack	PKM-REQ
36	M2M Key Request	PKM-REQ
37	M2M Key Reply	PKM-RSP
~~34~~38-255	*Reserved*	

Add new sections after 6.3.2.3.9.30

6.3.2.3.9.31 M2M Key Request Message

The MS sends this message to the BS to request the currently used multicast security parameters in case MS was not able to decrypt a secured multi-cast data.

Code: 36

Attributes are shown in Table 96a.

Table 96a—M2M Key Request Attributes

Attribute	Contents
MGID	The identifier of the M2M group of which the MS is a member of
HMAC/CMAC Digest	Message digest calculated using AK

The HMAC/CMAC Digest attribute shall be the final attribute in the message's attribute list. Inclusion of the HMAC/CMAC Digest attribute allows the MS and BS to authenticate the PKMv2 Key-Request message. The HMAC/CMAC Digest attribute's authentication key is derived from the AK.

6.3.2.3.9.32 M2M Key Reply Message

The BS sends this message to the MS to provide security information to derive the currently used multicast security key, M2MGTEK.

Code: 37

Attributes are shown in Table 96b.

Table 96b—M2M Key Reply Attributes

Attribute	Contents
MGID	The identifier of the M2M group of which the MS is a member of
MGSS	Randomly generated seed value for generating M2MGTEK
M2MGTEK_COUNT	The current M2MGTEK_COUNT value that the MS uses to derive the M2MGTEK
HMAC/CMAC Digest	Message digest calculated using AK

The HMAC/CMAC Digest attribute shall be the final attribute in the message's attribute list. Inclusion of the HMAC/CMAC Digest attribute allows the MS and BS to authenticate the PKMv2 Key-Request message. The HMAC/CMAC Digest attribute's authentication key is derived from the AK.

6.3.2.3.10 DSA-REQ message

Add the following new texts to the end of 6.3.2.3.10

When the DSA-REQ message is sent to an M2M device, the following TLV may be included:

MGID Tuple (see 11.13.46)

MGID that is added

6.3.2.3.13 DSC-REQ (DSC request) message

Add the following new texts to the end of 6.3.2.3.13

When the DSC-REQ message is sent to an M2M device, the following TLV may be included:

MGID Tuple (see 11.13.46)

MGID that is changed

6.3.2.3.26 DREG-CMD (de/reregister command) message

Add the following texts at the end of subclause 6.3.2.3.26

When the DREG-CMD message is sent to an M2M device, the following TLVs may be included:

M2M device-specific Idle mode timer

Length of the maximum interval between two consecutive location updates while the M2M device is in idle mode

Localized_Idle_Mode_Accepted flag

Indicator of the Localized Idle Mode for fixed M2M device

0: The M2M device enters the normal idle mode.

1: The M2M device enters the localized idle mode.

6.3.2.3.37 DREG-REQ (SS deregistration request) message

Add the following texts at the end of subclause 6.3.2.3.37

When the DREG-REQ message is sent to a base station, the following TLV may be included:

Localized_Idle_Mode_Accepted flag

Indicator of the Localized Idle Mode for fixed M2M device

0: The M2M device enters the normal idle mode.

1: The M2M device enters the localized idle mode.

6.3.2.3.51 MOB_PAG-ADV (BS broadcast paging) message

Change the contents of Table 172 as follows:

Table 172—MOB_PAG-ADV message format

Syntax	Size (bits)	Notes
...		

Table 172—MOB_PAG-ADV message format

Syntax	Size (bits)	Notes
For (j = 0; j < Num_MACs; j++) {	-	-
MS MAC Address hash	24	The hash is obtained by computing a CRC24 on the MS 48-bit MAC address. The polynomial for the calculation is 0x1864CFB
Action Code	2	Paging action instruction to MS 0b00 = No action required 0b01 = Perform ranging to establish location and acknowledge message 0b10 = Enter network 0b11 = Receiving multicast traffic
M2M network re-entry type	3	Indicate the network re-entry type for M2M device: 0b000: dedicated channel allocation for RNG-REQ 0b001: dedicated ranging channel allocation in MOB_PAG-ADV 0b010: dedicated ranging channel allocation in UL-MAP Extended IE 0b011: normal ranging channel 0b100-0b111: *reserved*
If (Action Code == 0b11) {		
Multicast Group ID (MGID)	15	The multicast group ID, which the multicast traffic is scheduled for
Multicast transmission start time (MTST)	TBD	Least significant TBD bits of the frame number in which the ABS starts sending DL multicast data. Shall be present when the MTST needs to be included in this message.
}		
M2M report code	1	Action instruction to M2M device 1: Indication for the M2M device to send the uplink report
Reserved	~~6~~2	-
}		
...		

Add new section after 6.3.2.3.97

6.3.2.3.98 MOB_MTE-IND (Multicast transmission end indication) message

The BS shall send a MOB_MTE-IND message to a group of M2M devices to indicate the end of multicast transmission. When an M2M device in idle mode receives the MOB_MTE-IND message, the M2M device may enter the paging unavailable interval as specified in 16.2.18.2.

Table 229a—MOB_MTE-IND message format

Syntax	Size (bits)	Notes
MOB_MTE-IND_Message_Format() {		
Management message type = TBD	8	-
CID	16	CID related to the multicast traffic
}		

6.3.9 Network entry and initialization

6.3.9.5 Initial ranging and automatic adjustments

6.3.9.5.1 Contention-based initial ranging and automatic adjustments

Change the paragraph as indicated

First, an SS shall synchronize to the DL and learn the UL channel characteristics through the UCD MAC management message. At this point, the SS shall scan the UL-MAP message to find an initial ranging interval. The BS shall allocate an initial ranging interval consisting of one or more transmission opportunities. For SC and OFDM PHY, the size of each transmission opportunity shall be as specified by the UCD TLV, Ranging Request Opportunity Size.

For SC and OFDM PHY, the SS shall put together a RNG-REQ message to be sent in an initial ranging interval. The duration of the burst carrying the RNG-REQ message shall be as specified in the Ranging Request Burst Size TLV (see 11.3.1). The CID field shall be set to the noninitialized SS value (zero). For the OFDM PHY, the initial ranging process may include a subchannelized mechanism specified in 8.3.7.2. For the OFDMA PHY, the initial ranging process shall begin by sending initial ranging CDMA codes on the UL allocation dedicated for that purpose (for more details see 6.3.10.3), instead of RNG-REQ messages sent on contention slots. An M2M device may perform ranging process using the initial ranging backoff window assigned by a MOB_PAG-ADV. The duration of this initial backoff window may be different from one assigned by UCD. This initial backoff window shall be only applied to the ranging process that is in response to the MOB_PAG-ADV message.

6.3.22 MS idle mode (optional)

6.3.22.6 BS Broadcast Paging message

Add the following texts at the end of subclause 6.3.22.6

MOB_PAG-ADV with M2M report code may be used to poll M2M devices for periodic uplink non-realtime data transmission for fixed M2M devices. When a M2M device receives the DREG-RSP message with the Transmission Type set to 1 and Max number of paging cycle TLV, the M2M device may wait for the MOB_PAG-ADV with M2M report code as long as Max number of paging cycle × paging cycle before sending uplink data. If the M2M device does not receive at least one MOB_PAG-ADV with M2M report code within Max number of paging cycle × paging cycle , it should not send the uplink.

Add new subclause 6.3.22.11

6.3.22.11 MS idle mode for M2M application

M2M device-specific Idle mode timer for an M2M device may be assigned during idle mode initiation. In this case, the DREG-CMD message includes M2M device-specific Idle mode timer as 11.14.1. A network entity administering idle mode activity for the M2M device shall maintain idle mode system timer corresponding to M2M device-specific Idle mode timer to retain the M2M device's service and operational information. When the M2M device receives the DREG-CMD message with M2M device-specific Idle mode timer, the M2M device shall periodically perform location update prior to the expiration of the M2M device-specific Idle mode timer. At every location update including the paging group location update, the M2M device-specific Idle mode timer is restarted.

Add new subclause 6.3.22.11.1

6.3.22.11.1 Network reentry from idle mode for M2M devices

BS may assign M2M specific ranging resources, including ranging code and ranging opportunity, dedicated for M2M devices. See 8.4.5.4.33 and 11.3.1, Table 671. In this case, M2M devices shall perform ranging for network (re-)entry using the dedicated ranging resources. If the BS does not assign dedicated ranging resources, M2M devices shall perform ranging for network (re-)entry using the ranging resources defined as specified in 6.3.10.3. BS may restrict ranging accesses from M2M devices by transmitting M2M Ranging Allocation UL-MAP Extended IE with access restriction indicator set to 1. If M2M devices receive M2M Ranging Allocation UL-MAP Extended IE with access restriction indicator set to 1, they shall not perform initial ranging for network reentry to this BS. Instead, the M2M devices may perform reselection of preferred BS or may resume initial ranging after the BS stops transmitting the M2M Ranging Allocation UL-MAP Extended IE with access restriction indicator set to 1. When the BS transmits an M2M Ranging Allocation UL-MAP Extended IE, the BS shall also transmit a UL-MAP IE with UIUC=12 identifying the same region as the M2M Ranging Allocation UL-MAP Extended IE and with the dedicated ranging indicator set to 1.

For individual paging, the dedicated ranging opportunities can be assigned by the BS to the M2M devices by using the TLV of CDMA code and transmission opportunity assignment in the MOB_PAG-ADV message, as specified in 6.3.2.3.51 and 11.17.1.

Based on the mobility and traffic characteristics of the M2M device, the BS shall indicate the M2M device the network re-entry scheme in MOB_PAG-ADV message.

If the network re-entry type is set to ‘0b000, the M2M device doesn't need to send CDMA code for ranging but decodes UL-MAP IE directly for slot allocation for RNG-REQ message. If the SS receives an UL-MAP containing a Fast Ranging IE at the UL-MAP IE offset that indicated in MOB_PAG-ADV, it shall proceed to send a unicast RNG-REQ on the allocated bandwidth.

If the network re-entry type is set to ‘0b001’, the BS shall allocate the dedicated ranging channel for M2M device in MOB_PAG-ADV message, the M2M device can find the dedicated CDMA code assignment and transmission opportunity offset in ‘CDMA code and transmission opportunity assignment’ of MOB_PAG-ADV message for ranging and network re-entry.

If the network re-entry type is set to ‘0b010’, the BS shall allocate the dedicated ranging channel for M2M device in UL-MAP Extended IE message.

If the network re-entry type is set to ‘0b011’, M2M device can only use the normal ranging channel.

Add new subclause 6.3.22.11.2

6.3.22.11.2 Idle mode optimizations for fixed M2M devices

Localized idle mode operation for idle mode M2M devices: a fixed M2M device in idle mode need not perform the paging group based update. To eliminate the need for paging group based update and allocating the unnecessary paging information (i.e., Paging Group ID, Paging Controller ID), a fixed M2M device may include Localized_Idle_Mode_Accepted flag set to 1 in the DREG-REQ message.

When a BS receives a DREG-REQ with Localized_Idle_Mode_Accepted flag set to 1, it does not inform the Paging Controller that the M2M device enters idle mode.

Then the BS sends DREG-CMD with Localized_Idle_Mode_Accepted flag set to 1 or 0. Localized_Idle_Mode_Accepted flag set to 1 indicates that the BS accepted M2M device's request. Then the M2M device transitions to idle mode and does not perform paging group based update.

Localized_Idle_Mode_Accepted flag set to 0, the M2M device enters the normal idle mode.

Add new subclause 6.3.34

6.3.34 Support of multicast operation for machine to machine application

Add new subclause 6.3.34.1

6.3.34.1 M2M multicast operation in idle mode

A BS may provide a multicast service for M2M devices in idle mode with or without requiring network reentry of the M2M devices. Before a BS sends DL multicast data, the BS may transmit the paging message including the multicast traffic indication to M2M devices during the paging listening intervals of the M2M devices. If an M2M device receives the paging message indicating multicast traffic reception without network reentry during its paging listening interval, the M2M device shall start receiving the DL multicast data without the idle mode termination.

The Multicast transmission start time TLV may be included in the paging message in order to indicate when the DL multicast data is sent by the BS. The value of Multicast transmission start time TLV shall be less than the start time of the next paging listening interval of the M2M devices receiving the MOB_PAG-ADV message. The M2M device may power down until the frame indicated by the Multicast transmission start time TLV in the MOB_PAG-ADV message.

When the multicast data transmission ends, the BS shall notify the end of multicast data transmission to the group of M2M devices by sending the AAI-MTE-IND message. Upon receiving the AAI-MTE-IND message, the M2M devices may enter the paging unavailable interval as specified in 16.2.18.2.

Add new subclause 6.3.35

6.3.35 Abnormal Power Down Reporting in Normal Mode

When a MS detects an abnormal power down event, it tries to send a RNG-REQ message with the Ranging Purpose Indication indicating that an abnormal or involuntary power down has occurred (bit 5 set to 1).

If the MS is in normal mode with uplink bandwidth already allocated and available, then it may use the available bandwidth to send this RNG-REQ message containing the Ranging Purpose Indication with value bit 5 set to 1.

If the MS is in normal mode but does not have available UL bandwidth, then it may use the procedure defined in 6.3.6 to request bandwidth. Upon receiving bandwidth allocation it may send the RNG-REQ message containing the Ranging purpose Indication with bit 5 set to 1.

Add new subclause 6.3.36

6.3.36 M2M small burst transmission

To support UL SMS from an M2M device in idle mode, two-round RNG-REQ/RSP are proposed as follows:

If the M2M device identifies the bandwidth allocation is enough for piggybacking SMS contents in RNG-REQ from the UL-MAP, it will omit the 1st round of RNG-REQ/RSP and send the RNG-REQ piggybacking SMS directly in second round of RNG-REQ.

The M2M device sends the RNG-REQ with M2M SMS Request TLV to indicate it has a SMS to send. If the BS receives the RNG-REQ with M2M SMS Request TLV successfully, it may accept or reject the request. In this case the BS shall transmit a RNG-RSP with SMS Response TLV with an action code instructing the M2M device how to proceed. If the BS accepts the SMS Request, the BS shall transmit a RNG-RSP with SMS Response TLV, with a Basic CID and a Temp CID Timer to be used for resource allocation for SMS transmission. For fixed M2M device, the M2M device can send RNG-REQ for SMS with the purpose indication for location update, but the paging related parameters can be removed from the RNG-REQ message to reduce the overhead because the BS is aware of its mobility information. This concludes the first round of RNG-REQ/RSP.

If the M2M device receives a RNG-RSP rejecting its SMS Request, it shall proceed according to the action code. If the M2M device receives a RNG-RSP accepting its SMS Request, it shall wait for bandwidth allocation for RNG-REQ with M2M SMS on its Basic CID and send a RNG-REQ with an M2M SMS TLV. If SMS packet is received successfully, the BS sends RNG-RSP with SMS confirmation to indicate. This concludes the second round of RNG-REQ/RSP.

The Basic CID is released once the M2M device receives the SMS Confirmation, or when the Temp CID Timer expires.

DL SMS TLV may be included in RNG-RSP message when the action code of MOB_PAG-ADV indicates location update.

For DL SMS transmission, the BS should send a Basic CID and a Temp CID Timer. When the M2M device receives the RNG-RSP with the DL SMS, a Basic CID and the Temp CID Timer, it may wait for bandwidth allocation for the RNG-REQ on the Basic CID. When SMS packet is received successfully, a RNG-REQ message is sent as a confirmation of the DL M2M SMS from the M2M device.

7. Security sublayer

7.2.2.2.10 Key hierarchy

Add the following texts at the end of the subclause 7.2.2.2.10 as indicated

Figure 240a outlines the M2M multicast authentication key hierarchy starting from the MAK.

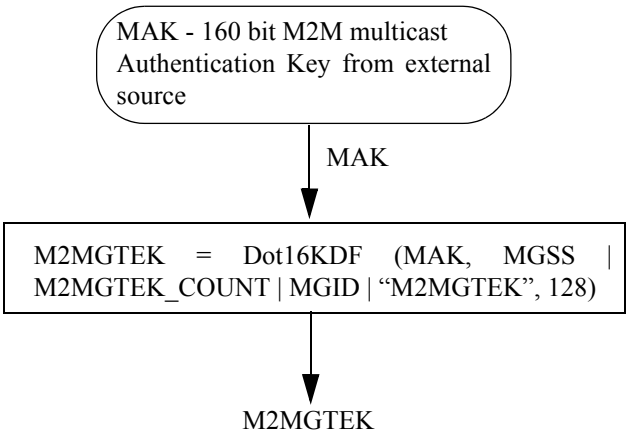

Figure 240a—M2MGTEK derivation from MAK

Add new section 7.2.2.2.14 as indicated

7.2.2.2.14 M2M Group Traffic Encryption Key (M2MGTEK)

The M2MGTEK is used to encrypt data packets of the multicast service, which is shared among all SSs that belong to the multicast group.

The M2MGTEK is generated based on the MAK, M2M service Group Security Seed (MGSS), MGID and the M2MGTEK_COUNT. The generation and transport of the MAK is outside the scope of the IEEE 802.16 standard. It is provided through means defined at higher layers.

The M2MGTEK is derived as the following:

M2MGTEK <= Dot16KDF(MAK, MGSS | M2MGTEK_COUNT | MGID | "M2MGTEK", 128)

- Here, the MAK is generated by network side, which is outside the scope of IEEE802.16 standard.
- Here, MGSS is a BS generated random seed value.
- Here, the M2MGTEK_COUNT indicates the index of the currently used M2MGTEK, which the M2M devices should apply to derive the M2MGTEK. The update of the M2MGTEK depends on the M2MGTEK_COUNT.
- Here, MGID is the M2M Group ID.

The M2MGTEK is updated when the 3 MSB of ROC concatenated with the frame number reaches 0x7FFFFF or an M2M device of the M2M group cancels its subscription. In case the 3 MSB of ROC con-

catenated with the frame number reaches 0x7FFFFF, the current M2MGTEK_COUNT is incremented by one by which the M2M devices perform local derivation to derive the new M2MGTEK.

If an M2M device cancels subscription from a group, the BS shall transmit a newly generated MGSS to each M2M device in the group via the unsolicited PKM-RSP message and initialize the M2MGTEK_COUNT. The MGSS value shall be encrypted within the PKM-RSP message. The BS shall exclude the unsubscribed M2M device from such security context update. For M2M devices in connected mode, the BS shall send the new security context via the unsolicited PKM-RSP message. For M2M devices in idle mode, the BS shall page the entire group (i.e., MGID) via the MOB_PAG-ADV message with 'Action Code' set to 0b10. For each M2M device that successfully performed network re-entry, the ABS shall send an unsolicited PKM-RSP message including the new MGSS.

If an M2M device is not able to decrypt an encrypted multicast data, the M2M device shall initiate a key update request by transmitting the PKM-REQ message to the BS. Here, the MS shall include its MGID. After authenticating the MS, the BS shall respond with the current MGSS and the M2MGTEK_COUNT that are in use via the PKM-RSP message.

Every M2M device that receives a PKM-RSP message with the new MGSS for updating the M2MGTEK shall respond with a PKM-REQ message for successful update acknowledgement.

7.2.2.2.14.1 Encrypted M2M multicast MPDU format

Unique initial counter and M2MGTEK pair is required across all messages. This subclause describes the initialization of the 128-bit initial counter, constructed from the frame number and a new 8-bit Rollover counter (ROC).

ROC shall be reset to zero upon obtaining a new M2MGTEK. The first 3 most significant bits of the ROC is the rollover counter for the frame number, i.e., when the frame number reaches 0x000000 (from 0xFFFFFF) it is incremented by 1 mod 8. The 5 least significant bits of ROC shall be allocated to M2M multicast MAC PDUs in such manner that no two M2M multicast MAC PDUs in the same frame using the same M2MGTEK have the same ROC value.

Using this method, up to 32 PDUs per frame using the same M2MGTEK can be supported. A new encryption key (M2MGTEK) is required every $2^3 \times 2^{24} = 2^{27}$ frames.

The PDU payload for AES-CTR encryption shall be prepended with the 8-bit ROC, i.e., the ROC is the 8 MSBs of the 32-bit nonce. The ROC shall not be encrypted.

Any tuple value of {AES Counter, KEY} shall not be used more than once for the purposes of encrypting a block. The MS and the BS shall ensure that a M2MGTEK_COUNT is incremented by one, and a new M2MGTEK is derived and ready for use before the 3 MSB of ROC concatenated with the frame number reaches 0x7FFFFF.

A 32-bit nonce is constructed as Table 279a.

Table 279a—Construction of 32-bit nonce

Byte number	0	1 3
Field	ROC	Frame number
Contents	ROC	24 bits of frame number

A 32-bit nonce NONCE = n0 | n1 | n2 | n3 is made of ROC and 24 bits frame number (see Table 279a). NONCE shall be repeated four times to construct the 128-bit counter block required by the AES-128 cipher. (initial counter = NONCE|NONCE|NONCE|NONCE). When incremented, this 16-byte counter shall be treated as a big endian number.

This mechanism can reduce per-PDU overhead of transmitting the full counter. At the most 2^{32} PDUs can be encrypted with a single M2MGTEK.

The plaintext PDU shall be encrypted using the active MGTEK derived from MAK, MGSS and M2MGTEK_COUNT, according to CTR mode specification. A different 128-bit counter value is used to encrypt each 128-bit block within a PDU.

The processing yields a payload that is 8 bits longer than the plaintext payload. See Figure 240b.

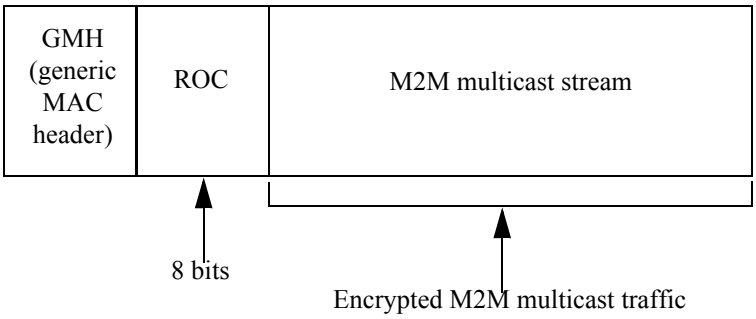

Figure 240b—M2M multicast MAC PDU ciphertext payload format

8. Physical layer (PHY)

8.4.5.4.4 UL-MAP Extended IE

8.4.5.4.4.1 UL-MAP Extended IE format

Modify Table 464 as indicated

Table 464—Extended UIUC code assignment for UIUC = 15

Extended UIUC (hexadecimal)	Usage
0x0	Power Control IE
0x1	*Reserved*
0x2	AAS UL IE
0x3	CQICH Allocation IE
0x4	UL Zone IE
0x5	UL-MAP Physical Modifier IE
0x6	*Reserved*
0x7	UL-MAP Fast Tracking IE
0x8	UL PUSC Burst Allocation in Other Segment IE
0x9	Fast Ranging IE
0xA	UL Allocation Start IE
0xB	UL Burst Receive IE
0xC	Dedicated Ranging Channel for M2M IE
0x~~C~~D ... 0xF	*Reserved*

Add new subclause 8.4.5.4.33 as indicated

8.4.5.4.33 M2M Ranging Allocation UL-MAP Extended IE format

The M2M Ranging Allocation UL-MAP Extended IE is used to indicate if the allocated ranging channel is used for M2M devices or to restrict new ranging accesses from M2M devices.

Table 512a—M2M Ranging Allocation UL-MAP Extended IE format

Syntax	Size (bit)	Notes
M2M Ranging Allocation UL-MAP Extended IE(){	-	-

Table 512a—M2M Ranging Allocation UL-MAP Extended IE format

Syntax	Size (bit)	Notes
Extended UIUC	4	M2M Ranging Allocation UL-MAP Extended = 0xC
Length	4	Length is TBD
Access restriction indicator	1	When this bit is set to 1, it indicates that M2M devices are not allowed to access this BS. When this bit is set to 0, this IE specifies the ranging allocation for M2M devices.
If (Access restriction indicator == 0) {		
OFDMA Symbol offset	8	-
Subchannel offset	7	-
No. OFDMA Symbols	7	-
No. Subchannels	7	-
Ranging Method	2	0b00: Initial ranging/Handover Ranging over two symbols 0b01: Initial ranging/Handover Ranging over four symbols 0b10-0b11: reserved
Dedicated ranging indicator	1	0: The OFDMA region and ranging method defined are used for the purpose of normal ranging 1: The OFDMA region and ranging method defined are used for the purpose of ranging using dedicated CDMA code and transmission opportunities assigned in the MOB_PAG-ADV message
}		
}		

11. TLV encodings

11.3 UCD management message encodings

11.3.1 UCD channel encodings

Add a new parameter at the end of Table 671 as indicated

Table 671—UCD channel encodings

Name	Type (1 byte)	Length	Value
M2M Ranging Region	31	6/12	The value of TLV consists of up to two concatenated sections (one section per Ranging method), each having the following structure: Bit 0: dedicated ranging indicator Bits 1-2: ranging method Bits 3-9: num subchannels Bits 10-16: num OFDMA symbols Bits 17-23: subchannel offset Bits 24-31: OFDMA symbol offset Bits 32-34: Parameter d that defines periodicity of 2^d frames Bits 35-39: Allocation phase expressed in frames, $0 \leq \text{Allocation Phase} < periodicity (= 2^d)$ Bits 40-47: *Reserved*

11.5 RNG-REQ management message encodings

Change the contents of Table 685 as indicated

Table 685—RNG-REQ message encodings

NAME	Type	Length	Value	PHY Scope
Ranging Purpose Indication	6	1	Bit 0: HO indication (when this bit is set to 1 in combination with other included information elements indicates the MS is currently attempting to HO or network reentry from idle mode to the BS) Bit 1: Location update request (when this bit is set to 1, it indicates MS action of idle mode location update process) Bit 2: Seamless HO indication (when this bit is set to 1 in combination with other included information elements indicates the MS is currently initiating ranging as part of the seamless HO procedure) Bit 3: Ranging Request for Emergency Call Setup (when this bit is set to 1, it indicates MS action of Emergency Call Process) Bit 4: MBS update. When this bit is set to 1, the MS is currently attempting to perform location update due to a need to update service flow management encodings for MBS flows. Bit 5: Abnormal Power Down Indication. When this bit is set to 1, MS indicates that an abnormal or involuntary power down occurs. Bits ~~5~~6-7: *Reserved*	-
M2M SMS Request	25	1	Bits 0-7: No. of bytes of SMS message	OFDMA
M2M SMS	26	Variable	M2M SMS message content up to 140bytes Padding bits to align boundary of byte.	OFDMA
M2M SMS Confirmation	27	1	Bit 0: SMS confirmation 0 - NACK 1 - ACK Bits 1-7: *Reserved*	OFDMA
Ranging Retries	28	1	The number of ranging retries in this ranging process Bits 0-1: Indicates the number of retrials in the channel ranging access as follows: 00 - Success in the first attempt 01 - Success in the second attempt 10 - Success in the third attempt 11 - Success in the 4th or later attempt	OFDMA
MIMO feedback information	41	1	Bit 0: Matrix indicator. This field suggests the preferred STC/MIMO matrix for the MS: 0b0: Matrix A 0b1: Matrix B Bits 1-4: DL effective CINR as defined in Table 520 Bits 5-7: *Reserved*	All

11.6 RNG-RSP management message encodings

Change the contents of Table 688 as indicated

Table 688—RNG-RSP message encodings

Name	Type(1byte)	Length	Value	PHY scope
...	...	...	...	...

M2M SMS Response	45	1	Bits 0-1: accept or reject SMS request
			0b0: reject
			0b1: accept
			If (reject) {
			Bits 2-3: action code
			0b00: network re-entry
			0b01-0b11: reserved
			} else {
			Reserved
			}
			Bits 4-7: *Reserved*
				OFDMA

Temp CID Timer	46	1	Life time duration for the Basic CID assigned by BS	OFDMA
M2M SMS Confir-mation	47	1	Bit 0: SMS confirmation b0 - NACK b1 -ACK Bits 1-7: *Reserved*	OFDMA
M2M SMS	48	Variable	M2M SMS message content up to 140 bytes Padding bits to align boundary of byte.	OFDMA

11.9 PKM-REQ/RSP management message encodings

Change the contents of Table 695 as indicated

Table 695—PKM attribute types

Type	PKM attribute
...	...
47	GKEK-Parameters
48	MIH Cycle
49	MIH Delivery Method and Status Code
53	M2M Multicast SA-Descriptor
54	M2MGTEK-Parameters
~~50~~55-255	*Reserved*

Add new subclause 11.13.46

11.9.43 M2M Multicast SA-Descriptor

The SA-Descriptor attribute is a compound attribute whose subattributes describe the properties of a security association (SA). These properties include the SAID, the SA type, the SA service type, and the cryptographic suite employed within the SA.

Type	Length	Value (compound)
53	Variable	The Compound field contains the subattributes shown in Table 710a

Table 710a—SA-Descriptor subattributes

Attribute	Contents
SAID	Security association identifier.
SA-Type	Type of security association.
SA Service Type	Service type of the corresponding security association type. This shall be defined only when SA type is Static SA or Dynamic SA.
Cryptographic-Suite	Cryptographic suite employed within the SA.

Add new subclause Table 11.9.44

11.9.44 M2MGTEK-Parameters

This attribute is a compound attribute, consisting of a collection of subattributes. These subattributes represent all the security parameters relevant to a particular generation of a M2MGTEK for encrypting multicast or broadcast data. A summary of the M2MGTEK-Parameters attribute format is shown below.

Type	Length	Value (compound)
54	Variable	The Compound field contains the subattributes shown in Table 710b

Table 710b—M2MGTEK-Parameters subattributes

Attribute	Contents
MGSS	Randomly generated seed value for generating M2MGTEK
M2MGTEK_COUNT	The current M2MGTEK_COUNT value that the MS uses to derive the M2MGTEK

Table 710b—M2MGTEK-Parameters subattributes

Attribute	Contents
ROC	8-bit Rollover counter (ROC)

11.13 Service flow management encodings

Add new subclause 11.13.46

11.13.46 MGID field

The value of this field specifies MGID that is used for the associated flow. During connected mode, the MGID may be added by DSA-REQ message and may be changed by DSC-REQ message.

Name	Type	Length	Value	Scope
MGID	[145/146].57	2	Bits 0-14: Indicates MGID; Bit 15: Padding, Will be set to 0	DSA-REQ DSC-REQ

11.14 DREG-CMD/REQ message encodings

Add new subclause 11.14.1

11.14.1 M2M device-specific Idle mode timer

Name	Type	Length	Value	Scope
M2M device-specific Idle mode timer	53	3	Length of the maximum interval between two consecutive location updates while the M2M device is in idle mode	DREG-CMD
Transmission Type	54	1	Bit 0: allowed to send data only after receiving a paging message with M2M report code Bits 1-7: *reserved.*	DREG-CMD
Max number of paging cycle	55	8	This is max number of paging cycle for M2M device to wait for MOB_PAG-ADV with M2M report code. The unit is the duration of the paging cycle.	DREG-CMD

11.17 MOB_PAG-ADV management message encodings

Insert new subclause 11.17.5

11.17.5 M2M group paging parameter

The following M2M group paging parameter TLV may be included in MOB_PAG-ADV message.

Name	Type	Length	Value	Scope
M2M group paging parameter	156	Variable	Compound TLV to be used in M2M group paging operation	MOB_PAG-ADV

The following TLV element shall appear in each M2M group paging parameter TLV.

Name	Type	Length	Value
MGID	156.1	2	Bits 0-14: Indicates M2M Group ID; Bit 15: Padding, Will be set to 0
Action code	156.2	1	Bits 0-1: Indicates Action code for the M2M Group ID 0b00 - Performing network reentry 0b01- Performing location update 0b10 - Receiving multicast traffic 0b11- *Reserved* Bits 2-7: Padding, Will be set to 0

The following TLV element may appear in each M2M group paging parameter TLV.

Name	Type	Length	Value
Multicast transmission start time (MTST)	156.3	1	Least significant 8 bits of the frame number in which the ABS starts sending DL multi-cast data