



IEEE Standard for Low-Rate Wireless Networks

Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques

IEEE Computer Society

Developed by the
LAN/MAN Standards Committee

IEEE Std 802.15.4z™-2020
(Amendment to IEEE Std 802.15.4™-2020)

IEEE Standard for Low-Rate Wireless Networks

Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques

Developed by the
LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 4 June 2020

IEEE SA Standards Board

Abstract: This amendment enhances the UWB PHYs with additional coding options and improvements to increase the integrity and accuracy of ranging measurements. It also enhances the MAC to support control of time-of-flight ranging procedures and exchange ranging related information between the participating ranging devices.

Keywords: amendment, double-sided two-way ranging, DS-TWR, enhanced ranging device, ERDEV, HRP UWB PHY, HRP-ERDEV, IEEE 802.15.4™, IEEE 802.15.4z™, low power, low-rate wireless networks, LRP UWB PHY, LRP-ERDEV, multi-node ranging, precision ranging, ranging device, RDEV, RF, RFID, real time location systems, RTLS, single-sided two-way ranging, SS-TWR, time of flight, TOF, TOF integrity, two-way ranging, TWR, ultra wideband, UWB, wireless specialty networks, WSN

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2020 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 25 August 2020. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-6798-8 STD24237
Print: ISBN 978-1-5044-6799-5 STDPD24237

IEEE prohibits discrimination, harassment and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.” They can also be obtained on request from IEEE or viewed at <https://standards.ieee.org/ipr/disclaimers.html>.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (“IEEE SA”) Standards Board. IEEE (“the Institute”) develops its standards through a consensus development process, approved by the American National Standards Institute (“ANSI”), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

Secretary, IEEE SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854 USA

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document 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

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted 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 these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents 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. A current 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.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

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 SA Website at <https://ieeexplore.ieee.org> or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at <https://standards.ieee.org>.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website at the following URL: <https://standards.ieee.org/findstds/errata/index.html>. Users are encouraged to check this URL for errata periodically.

Patents

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 by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent 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.

Essential Patent Claims may exist for which a Letter 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 provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was completed, the IEEE 802.15 Working Group had the following membership:

Robert F. Heile, *IEEE 802.15 Working Group Chair*
Rick Alfvén, *IEEE 802.15 Working Group Vice-Chair*
Patrick W. Kinney, *IEEE 802.15 Working Group Vice-Chair, IEEE 802.15 Working Group Secretary*
James P. K. Gilb, *IEEE 802.15 Working Group Technical Editor*
Benjamin A. Rolfe, *IEEE 802.15 Working Group Treasurer*

Tim Harrington, *IEEE 802.15.4z Task Group Chair*
Benjamin A. Rolfe, *IEEE 802.15.4z Task Group Vice-Chair and Secretary*
Billy Verso, *IEEE 802.15.4z Task Group Technical Editor*

Hendrik Ahlendorf	Roger Hislop	Jaroslav Niewczas
Koorosh Akhavan	Jay Holcomb	Paul Nikolich
Bernd Baer	Oliver Holland	Philip Orlik
David Barras	Iwao Hosako	Aditya Padaki
Tuncer Baykas	Brima Ibrahim	Clark Palmer
Philip Beecher	Tetsushi Ikegami	Glenn Parsons
Friedbert Berens	Yeong Min Jang	Charles Perkins
Harry Bims	Seongah Jeong	Albert Petrick
Lennert Bober	Seong-Soon Joo	Joe Polland
Monique Brown	Volker Jungnickel	Clinton Powell
Chris Calvert	Juha Juntunen	Demir Rakanovic
Radhakrishna Canchi	S. G. Karthik	Ivan Reede
Jaesang Cha	Paul Kettle	Joerg Robert
Soo-Young Chang	Shoichi Kitazawa	Alessandra Rocha
Matthew Chang	Tero Kivinen	Ren Sakata
Clint Chaplin	Daniel Knobloch	Ruben E. Salazar Cardozo
Sangsung Choi	Ryuji Kohno	Ioannis Sarris
Nathan Clanney	Fumihide Kojima	Peter Sauer
Michael G. Cotton	Ann Krieger	Nikola Serafimovski
Boris Danev	Thomas Kuerner	Daoud Serang
Luc Darmon	Jack Lee	Kunal Shah
Hendricus De Ruijter	Mingyu Lee	Tushar Shah
Brandon Dewberry	Frank Leong	Menashe Shahar
Anthony Fagan	Huan-Bang Li	Stephen Shellhammer
Robert Finch	Zheda Li	Guy Simpson
Michael Gagne	Sang-Kyu Lim	William Smith
Matthew Gillmore	Thomas Lorbach	Frederick Smith
Tim Godfrey	Masood Maqbool	Gary Stuebing
Jianlin Guo	Vinayagam Mariappan	Don Sturek
Joachim Hammerschmidt	Alejandro Marquez	Craig Tedrow
Shinsuke Hara	Gianfranco Miele	Johannes Wechsler
Hiroshi Harada	Apurva Mody	Brian Weis
Chris Hartman	Ayman Naguib	Peter Yee
Christopher Hett	Kathleen Nelson	Shaun Yu

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

Thomas Alexander	Werner Hoelzl	Robert Robinson
David Barras	Brima Ibrahim	Benjamin A. Rolfe
Philip E. Beecher	Raj Jain	Ruben E. Salazar Cardozo
Harry Bims	SangKwon Jeong	Shigenobu Sasaki
Nancy Bravin	Srinivas Kandala	Naotaka Sato
Vern Brethour	S. G. Karthik	Peter Sauer
Demetrio Bucaneg, Jr.	Stuart Kerry	James Schuessler
William Byrd	Yongbum Kim	Kunal Shah
Paul Cardinal	Patrick W. Kinney	Tushar Shah
Juan Carreon	Tero Kivinen	Robert Stacey
Pin Chang	Jarkko Knecht	Dorothy Stanley
Clint Chaplin	Daniel Knobloch	Thomas Starai
Charles Cook	Jan Kruys	Gary Stuebing
Boris Danev	Yasushi Kudoh	Don Sturek
Hendricus De Ruijter	Hyeong Ho Lee	Mark Sturza
Brandon Dewberry	Mingyu Lee	Bo Sun
Igor Dotlic	Wookbong Lee	Mark-Rene Uchida
Edward Eckert	Frank Leong	Aditya V. Padaki
Anthony Fagan	Zheda Li	Dmitri Varsanofiev
Michael Fischer	Yong Liu	Billy Verso
Avraham Freedman	Thomas Lorbach	George Vlantis
James P. K. Gilb	Michael Mc Laughlin	Lisa Ward
Matthew Gillmore	Michael McInnis	Karl Weber
Robert Golshan	Ayman Naguib	Scott Willy
Randall Groves	Nick S. A. Nikjoo	Andreas Wolf
Rainer Hach	Tetsu Nishimura	Chi Xu
Joachim Hammerschmidt	Bansi Patel	Shang-Te Yang
Timothy Harrington	Dev Paul	Kangjin Yoon
Robert F. Heile	Arumugam Paventhan	Yu Yuan
Jerome Henry	Clinton Powell	Oren Yuen
Marco Hernandez	Maximilian Riegel	Sven Zeisberg

When the IEEE SA Standards Board approved this standard on 4 June 2020, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse	David J. Law	Mehmet Ulema
Doug Edwards	Howard Li	Lei Wang
J. Travis Griffith	Dong Liu	Sha Wei
Grace Gu	Kevin Lu	Philip B. Winston
Guido R. Hiertz	Paul Nikolic	Daidi Zhong
Joseph L. Koepfinger*	Damir Novosel	Jingyi Zhou
	Dorothy Stanley	

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.15.4z-2020, IEEE Standard for Low-Rate Wireless Networks—Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques.

This amendment of IEEE Std 802.15.4-2020 specifies enhancements and enhanced modes of operation for the HRP UWB PHY and the LRP UWB PHY and associated ranging techniques in the MAC. The PHY enhancements include facilities to improve the integrity and accuracy of the ranging measurements. The MAC enhancements include specification of information element definitions to facilitate ranging information exchange, and changes to support the PHY enhancements.

These enhancements meet the needs of a wider set of applications where the integrity and accuracy of distance measurement is important.

The standard is widely used in a variety of applications that employ the ranging capabilities enabled by the UWB PHYs specified by IEEE Std 802.15.4-2020. Current users and product manufacturers have identified the need for improved efficiency, integrity, and accuracy of the existing ranging measurement methods in order to expand the usefulness of the standard for applications such as RFID and automotive, in particular, automotive remote control, and similar personal devices. These enhancements are also expected to open up new areas of application.

Contents

2.	Normative references	13
3.	Definitions, acronyms, and abbreviations.....	14
3.1	Definitions	14
3.2	Acronyms and abbreviations	14
5.	General description	15
5.7	Functional overview	15
5.7.3	Frame structure	15
6.	MAC functional description	16
6.2	Channel access.....	16
6.2.11	Beacon-enabled ranging with ERDEV	16
6.7	Transmission, reception, and acknowledgment.....	17
6.7.2	Reception and rejection	17
6.7.4	Use of acknowledgments and retransmissions	17
6.9	Ranging, relative positioning, and localization	17
6.9.1	Ranging requirements measurements	17
6.9.2	Set-up activities before a ranging exchange	25
6.9.3	Finish-up activities after a ranging exchange	25
6.9.4	Managing DPS and DCS	25
6.9.5	The basic ranging exchange.....	27
6.9.6	Ranging procedures	28
6.9.7	Multi-node ranging	37
6.9.8	Authenticated challenge-response ranging	59
6.9.9	Ranging message non-receipt exchange	72
6.9.10	Ranging ancillary information	72
6.9.11	Multiple Message Receipt Confirmation.....	73
7.	MAC frame formats.....	74
7.2	General MAC frame format.....	74
7.2.11	FCS field.....	74
7.4	IEs	74
7.4.2	Header IEs.....	74
7.4.4	Nested IE.....	75
7.5	MAC commands	98
7.5.1	Command ID field	98
7.5.31	Ranging Verifier command	98
7.5.32	Ranging Prover command	99
8.	MAC services	100
8.2	MAC management service.....	100
8.2.1	Primitives supported by the MLME-SAP interface.....	100
8.2.5	Communications notification primitives	100
8.2.10	Primitives for specifying the receiver enable time	100
8.2.15	Primitives for specifying dynamic channel and preamble selection.....	105
8.2.16	Primitives for channel sounding	107
8.2.17	Primitives for ranging calibration	107

8.2.18	Primitives for Beacon Generation.....	108
8.2.25	RIT data commands	108
8.2.27	Primitives for specifying STS parameters	109
8.3	MAC data service	111
8.3.1	General.....	111
8.3.2	MCPS-DATA.request.....	111
8.3.3	MCPS-DATA.confirm.....	114
8.3.4	MCPS-DATA.indication	117
8.3.7	ACRR verifier primitives.....	123
8.3.8	ACRR prover primitives	128
8.4	MAC constants and PIB attributes.....	132
8.4.3	MAC PIB attributes	132
10.	General PHY requirements	133
10.1	General.....	133
10.1.2	Operating frequency range.....	133
10.1.3	Channel assignments.....	133
10.2	General radio specifications.....	134
10.2.8	Clear channel assessment (CCA).....	134
10.3	Ranging capable PHY	134
10.3.1	General.....	134
10.3.2	Distance commitment on PSDU	134
11.	PHY services	136
11.2	PHY constants.....	136
11.3	PHY PIB attributes	136
15.	HRP UWB PHY	140
15.1	General.....	140
15.2	HRP UWB PPDU format	140
15.2.1	General.....	140
15.2.2	PPDU encoding process.....	141
15.2.6	SHR field	141
15.2.7	PHR field	143
15.2.8	PHY Payload field	145
15.2.9	Scrambled timestamp sequence (STS) field	145
15.3	Modulation.....	148
15.3.3	FEC	148
15.3.4	HRP-ERDEV modulation in HPRF mode.....	149
15.4	RF requirements.....	153
15.4.4	Baseband impulse response	153
15.4.6	Chip rate clock and chip carrier alignment.....	154
15.7	HRP-ERDEV parameter sets	154
18.	LRP UWB PHY specification	157
18.1	Overview.....	157
18.2	LRP UWB PHY symbol structure	158
18.2.1	Overview.....	158
18.2.5	Dual-frequency LRP UWB PHY symbol structure.....	159
18.2.6	Variable pulse repetition period (PRP)	159
18.3	LRP UWB SHR	160

18.3.2	LRP UWB SHR preamble	160
18.3.3	LRP UWB SHR SFD.....	161
18.5	LRP UWB PSDU.....	162
18.5.1	General.....	162
18.5.2	PSDU in enhanced payload capacity (EPC) mode	162
18.6	LRP UWB location enhancing information postamble	163
18.7	LRP UWB transmitter specification	164
18.7.1	Pulse shape.....	164
18.7.2	Pulse timing	164
18.7.3	Transmit PSD mask	164
18.8	LRP UWB transmit and receive timing requirements	168
18.8.1	Fixed reply time	168
18.8.2	Turnaround times	168
Annex A (informative) Bibliography		169
Annex D (informative) Protocol implementation conformance statement (PICS) proforma.....		170
Annex H (informative) STS generation.....		171

IEEE Standard for Low-Rate Wireless Networks

Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques

(This amendment is based on IEEE Std 802.15.4™-2020.)

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

The editing instructions are shown in ***bold italic***. Four editing instructions are used: change, delete, insert, and replace. ***Change*** is used to make 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. Deletions and insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. ***Replace*** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.¹

¹ Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

2. Normative references

Insert the following new normative references in alphabetical order:

IEEE Std 802.15.9TM-2016, IEEE Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams.²

ISO/IEC 7816-4:2013, Identification cards—Integrated circuit cards—Part 4: Organization, security and commands for interchange.³

ISO/IEC 7816-5:2004, Identification cards—Integrated circuit cards—Part 5: Registration of application providers.

JIS X 6319-4:2016, Specification of implementation for integrated circuit(s) cards—Part 4: High speed proximity cards.⁴

²IEEE publications are available from The Institute of Electrical and Electronics Engineers (<https://standards.ieee.org/>).

³ISO publications are available from the International Organization for Standardization (<https://www.iso.org/>) and the American National Standards Institute (<https://www.ansi.org/>).

⁴JIS standards are available from The Japanese Standards Association, (<https://www.jsa.or.jp/>).

3. Definitions, acronyms, and abbreviations

3.1 Definitions

Insert the following new definitions in alphabetical order:

scrambled timestamp sequence (STS): A sequence of pseudo-randomized pulses generated using a deterministic random bit generator (DRBG).

STS key: A parameter that is part of the seed input to the STS generating DRBG and which may be privileged information or not depending on the application needs.

3.2 Acronyms and abbreviations

Insert the following new acronyms/abbreviations in alphabetical order:

AOA	angle of arrival
BPRF	base pulse repetition frequency
DCS	dynamic channel selection
DRBG	deterministic random bit generator
DS-TWR	double-sided two-way ranging
EPC	enhanced payload capacity
ERDEV	enhanced ranging capable device
HPRF	higher pulse repetition frequency
HRP-ERDEV	high rate pulse repetition frequency UWB PHY based enhanced ranging capable device
LRP-ERDEV	low rate pulse repetition frequency UWB PHY based enhanced ranging capable device
OWR	one-way ranging
PBFSK	pulsed binary frequency shift keying
PRP	pulse repetition period
PSR	preamble symbol repetitions
RBS	ranging beacon slot
RCM	ranging control message
RSTU	ranging scheduling time unit
SP3	scrambled timestamp sequence packet configuration option three
SS-TWR	single-sided two-way ranging
STS	scrambled timestamp sequence
TDOA	time difference of arrival
TOF	time of flight
TWR	two-way ranging

5. General description

5.7 Functional overview

5.7.3 Frame structure

Change paragraphs two and three of 5.7.3 as follows:

The MAC frames are passed to the PHY as the PSDU, which becomes the PHY payload. The typical structure of a PHY protocol data unit (PPDU) is illustrated in Figure 5-7.

The format of the SHR, ~~and~~ PHR, PPSU and any other PHY specific fields is defined for each of the PHYs in their respective clause.

6. MAC functional description

6.2 Channel access

Insert new subclause 6.2.11 after 6.2.10 as follows:

6.2.11 Beacon-enabled ranging with ERDEV

Support of beacon-enabled ranging for an enhanced ranging capable device (ERDEV) is optional. The ranging time structure for beacon-enabled ERDEV is shown in Figure 6-13a. The ranging time structure is characterized by repeating ranging beacons, where a ranging beacon is an Enhanced Beacon frame containing the Ranging Descriptor IE (RD IE) specified in 7.4.4.54.

The beacon interval of the ranging time structure is the time between two ranging beacons. The ranging time structure is composed of the ranging management period and the ranging period. The ranging management period is comprised of ranging beacon slots (RBS). Each RBS has a duration specified in the ranging beacon (in multiples of the ranging scheduling time units (RSTU) defined in 6.9.1.5). The RBS duration needs to be sufficient to allow transmission of a ranging beacon. The ranging beacon occupies RBS number zero. The ranging period consists of one or more ranging slots (see 6.9.7). The RD IE in the ranging beacon conveys the beacon interval value, information on the usage of the ranging management period, and the beginning of the ranging period.

The ranging management period may have one or more ranging contention access period(s) (RCAP) and one or more ranging contention free period(s) (RCFP). Each RCFP and RCAP is one or more RBS. The RCAP and RCFP may be interleaved in the ranging management period. The ranging management period may or may not be present in a given beacon interval. The channel access for slots in an RCAP is contention based and for slots in an RCFP is schedule based.

The ranging period is structured as defined in 6.9.7.2 and 6.9.7.3. The ranging period begins with a ranging control message (RCM), which configures the ranging period. The ranging period may have more than one RCM. The ranging period may last until the next ranging beacon or could end before the next ranging beacon. The ranging period may or may not be present in a given beacon interval.

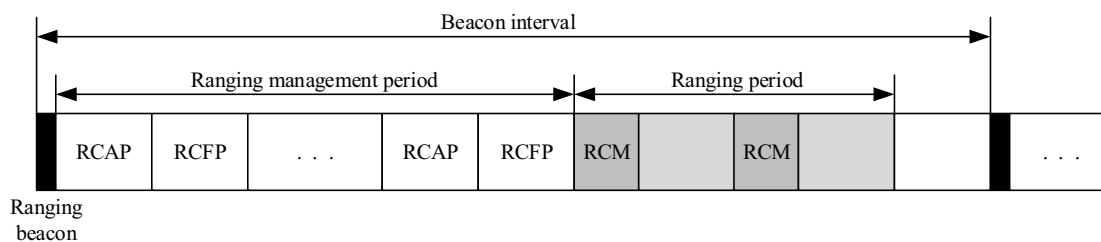


Figure 6-13a—Ranging time structure for beacon-enabled ranging with ERDEV

6.7 Transmission, reception, and acknowledgment

6.7.2 Reception and rejection

Insert the following paragraph at the start of 6.7.2:

When a device is configured to use raw mode using the RawMode parameter of the MCPS-RANGING-VERIFIER.request or MCPS-RANGING-PROVER.request primitives, the frame is processed without conducting any of the filtering described in this subclause.

Insert the following paragraph at the end of 6.7.2:

In the case of an HRP-ERDEV configured to use SP3 format packets (where the packet does not include a MHR, MFR, PHR, or data payload) the reception of a packet shall be treated differently from a normal data packet. For an unintended recipient expecting a normal data packet, the lack of PHR in the received packet shall cause the MAC sublayer to discard the received packet. For a receiver expecting an SP3 packet, depending on the implementer's choice, the MAC or PHY sublayer shall either accept the received packet if and only if the STS sequence in the received frame matches the expected STS sequence, or accept the received packet and notify the next higher layer of its arrival with the RangingStsFom set accordingly. In the latter case the higher layers can reject the packet if the STS in the received packet does not match the expected STS. The packet is processed without conducting any of the filtering described in this subclause.

6.7.4 Use of acknowledgments and retransmissions

6.7.4.3 Acknowledgment

Insert the following paragraph at the end of 6.7.4.3:

The acknowledgment transmission in response to an RFRAME shall be contained in an RFRAME.

Change the titles of 6.9 and 6.9.1, make the text of 6.9.1 into a new subclause 6.9.1.1, and change it as follows:

6.9 Ranging, relative positioning, and localization

6.9.1 Ranging ~~requirements~~ measurements

6.9.1.1 Overview

Support for ranging is optional. A device that supports ranging is called a ranging-capable device (RDEV). An RDEV shall support the ranging counter described in 6.9.1.3 and the figure of merit (FoM) described in 6.9.1.7. An RDEV may support optional crystal characterization described in 6.9.1.6 and the optional dynamic preamble code and channel selection (DPS) described in "Applications of IEEE Std 802.15.4" [B3]. RDEVs produce ranging results, used by higher layers to compute the ranges between devices. These ranging results may include transmit and receive ranging counter values, ranging FoM, angle of arrival (AOA) information, ranging tracking interval, and ranging tracking offset values.

~~Ranging is an optional feature.~~ This standard includes optional features to support relative positioning and localization. Accurate location may be achieved by a ranging-capable device (RDEV) using one of the ultra wideband (UWB) PHYs defined in this standard that provide the capability to accurately determine packet reception and transmission times. With accurate message timestamping, techniques such as two-way ranging (TWR) time of flight (TOF) can give very accurate estimates of relative separation distance between

two devices. Similarly, an accurate location estimate for a mobile device can be determined, for example, when its distance from a number of fixed devices (of known location) is ascertained.

The UWB PHYs specified in Clause 15 and Clause 18 optionally include facilities to enhance ranging, and these ERDEVs are referred to as the high rate pulse repetition frequency UWB PHY based enhanced ranging capable device (HRP-ERDEV) and the low rate pulse repetition frequency UWB PHY based enhanced ranging capable device (LRP-ERDEV), respectively.

The HRP-ERDEV incorporates an STS, see 15.2.9, generated by an AES-128 based deterministic random bit generator (DRBG). Only valid transmitters and receivers know the correct seed to generate the sequence for transmission and for reception to cross correlate and accumulate to produce a channel impulse response estimate from which to accurately determine the receive time.

The LRP-ERDEV supports challenge-response authenticated ranging with distance commitment on secret data payload. These ranging schemes are described in 6.9.8.

The fundamental measurements for ranging are achieved using a ~~Data frame Ack frame sequence~~ transmitted frame and a response frame. For example, a ranging exchange may consist of a Data frame and its acknowledgment. As another example, the response could be a Data frame. A frame used for a ranging measurement ~~The Data frame has the Ranging field set to indicate ranging and~~ is referred to as a ranging frame (RFRAME). Generally, an RFRAME is indicated by the Ranging field being set in the PHR, however as described in 15.2, the HRP-ERDEV has a packet configuration where the PPDU has no PHR (or data) but consists solely of the SHR and STS. This is STS packet configuration three (SP3). SP3 packets are treated as RFRAMES.

Ranging capabilities are enabled in ~~an RDEV a ranging-capable device (RDEV)~~ with the MCPS-DATA.request primitive and with the MLME-RX-ENABLE.request primitive. Whenever ranging is enabled in an RDEV, the RDEV delivers accurate transmit and receive time ~~timestamp~~ reports to the next higher layer as a result of events at the device antenna. The ~~times that are reported are timestamp that is reported~~ is measured relative to the ranging marker (RMARKER). For all PHYs the RMARKER is defined to be the time when the beginning of the first symbol following the SFD of the PHR of the RFRAME is at the local antenna. For UWB PHYs this shall be the peak pulse location associated with the first chip following the SFD. An HRP-ERDEV can use the STS to determine time of arrival and then derive the RMARKER time.

The relative positioning and locating methods supported by this standard are: single-sided two-way ranging (SS-TWR), double-sided two-way ranging (DS-TWR) and one-way ranging (OWR) for the time difference of arrival (TDOA) localization method.

In a typical implementation, the transmit and receive time reports will be captured by the transmitter and receiver, and then adjusted to account for the time difference between the internally captured time and the time the RMARKER actually launches or arrives at the antenna. These offsets are separately defined for transmitter and receiver as the configurable PIB attributes phyTxRmarkerOffset and phyRxRmarkerOffset.

The TxRangingCounter and RxRangingCounter values within the RangingReportDescriptor (defined in Table 8-90a) parameter of the MCPS-DATA.confirm and MCPS-DATA.indication primitives report RMARKER transmit and receive times as specified in 8.3.

The next higher layer can estimate the relative clock offset between the remote transmitter and the local reference clock at the receiver based on the reported SRMARKER receive ranging counter values for one or more STS segments. This allows estimation of individual clock offsets per subsystem in case different subsystems are used to transmit or receive different STS segments, e.g., in ranging nodes featuring antenna

diversity. For example, to determine the relative clock offset via the first STS segment, the following calculation can be used:

$$\frac{f_{\text{ref.remote}}}{f_{\text{ref.local}}} = \frac{L_{\text{segment.ideal}}}{\text{RxS1RangingCounter} - \text{RxS0RangingCounter}}$$

Insert new subclauses 6.9.1.2 through 6.9.1.7 before 6.9.2 as follows:

6.9.1.2 Ranging and localization methods

6.9.1.2.1 Preface

The ranging and localization methods supported by RDEVs and ERDEVs are based on the time-stamping capability. The three main time-based techniques for performing ranging and localization are as follows:

- SS-TWR, described in 6.9.1.2.2.
- DS-TWR, described in 6.9.1.2.3.
- OWR/TDOA, described in 6.9.1.2.5.

The following nomenclature is used:

- Initiator: the RDEV that starts ranging exchange by sending the first RFRAME in the exchange.
- Responder: the RDEV that responds to the ranging initiation RFRAME.

6.9.1.2.2 Single-sided two-way ranging (SS-TWR)

SS-TWR involves a measurement of the round-trip delay of a single message from one device to another and a response sent back to the original device. The operation of SS-TWR is as shown in Figure 6-47a, where device A initiates the exchange and device B responds to complete the exchange and T_{prop} is the propagation time of the RMARKER between the devices.

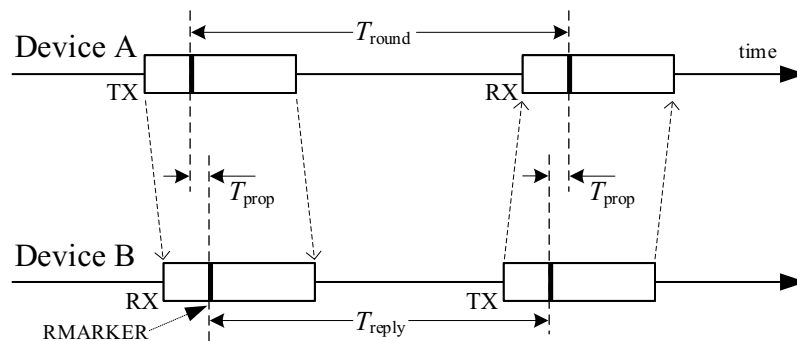


Figure 6-47a—SS-TWR

Each device precisely measures the transmission and reception times of the message frames, and so can calculate times T_{round} and T_{reply} by simple subtraction. Hence, the resultant TOF may be estimated as $\hat{T}_{\text{prop}}$ by the equation:

$$\hat{T}_{\text{prop}} = \frac{1}{2}(T_{\text{round}} - T_{\text{reply}})$$

The times T_{round} and T_{reply} are measured independently by device A and B using their local clocks, which both have some clock frequency offset error e_A and e_B , respectively, from their nominal frequency. Therefore, the resulting TOF estimate has a considerable error that increases as the reply times get larger, as explained in “Applications of IEEE Std 802.15.4” [B3]. However if the receiver of device A has the capability to measure the relative clock offset between itself and the remote device B transmitter, C_{offs} , then this may be used to adjust the reported T_{reply} value to improve the accuracy of the TOF estimate using the equation:

$$\hat{T}_{\text{prop}} = \frac{1}{2}(T_{\text{round}} - T_{\text{reply}} - (1 - C_{\text{offs}}))$$

When the receiver has the capability to measure the relative clock frequency offset this is reported via the RangingTrackingInterval and RangingOffset parameters of the MCPS-DATA.confirm or MCPS-DATA.indication primitives.

When employing SS-TWR, for the TOF to be calculated at device A, device A needs the reply time T_{reply} employed by device B. When T_{reply} is determined by device B after its transmission, an additional message is necessary to bring this value to device A, as shown in Figure 6-48a and described in 6.9.6.3. When T_{reply} can be accurately predicted by device B before its transmission, the value can be embedded in the reply message itself, as shown in Figure 6-48b and described in 6.9.6.4. Alternatively, if device B has the ability to always reply with sufficiently accurate constant or pre-known reply time, it obviates the need for any transfer of T_{reply} as part of the ranging exchange, as described in 6.9.6.5.

6.9.1.2.3 Double-sided two-way ranging (DS-TWR)

DS-TWR is an extension of SS-TWR in which two round-trip time measurements are used and combined to give the TOF result with a reduced error in the presence of uncorrected clock frequency offset even for quite long response delays. The operation of DS-TWR is shown in Figure 6-47b, where device A initiates the first round-trip time measurement to which device B responds, after which device B initiates the second round-trip time measurement to which device A responds completing the full DS-TWR exchange and T_{prop} is the propagation time of the RMARKER between the devices.

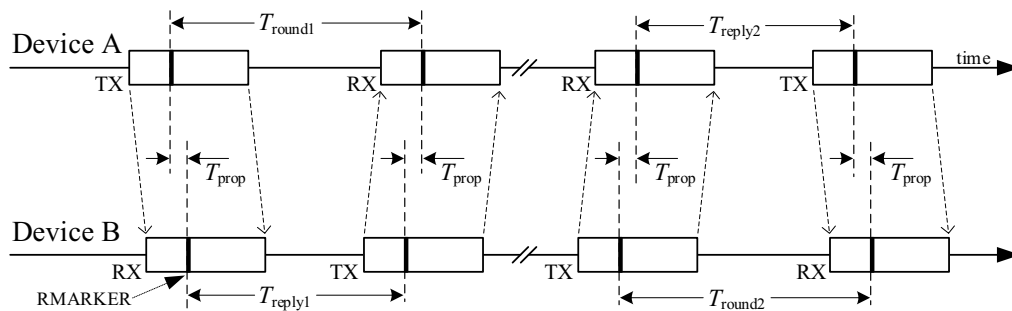


Figure 6-47b—DS-TWR

Each device precisely measures the transmission and reception times of the messages, and the resultant TOF may be estimated as $\hat{T}_{\text{prop}}$ by the equation:

$$\hat{T}_{\text{prop}} = \frac{(T_{\text{round1}} \times T_{\text{round2}} - T_{\text{reply1}} \times T_{\text{reply2}})}{(T_{\text{round1}} + T_{\text{round2}} + T_{\text{reply1}} + T_{\text{reply2}})}$$

NOTE—This formula does not require symmetric reply times. The typical clock induced error is in the low picosecond range even with 20 ppm crystals and asymmetric response times. The derivation of this formula and the error calculation can be found in IEEE Std 802.15.8™-2017, Annex D, subclause D2 [B7a].

6.9.1.2.4 DS-TWR with three messages

The four messages of DS-TWR, shown in Figure 6-47b, can be reduced to three messages by using the reply of the first round-trip time measurement as the initiator of the second round-trip time measurement. This is shown in Figure 6-47c.

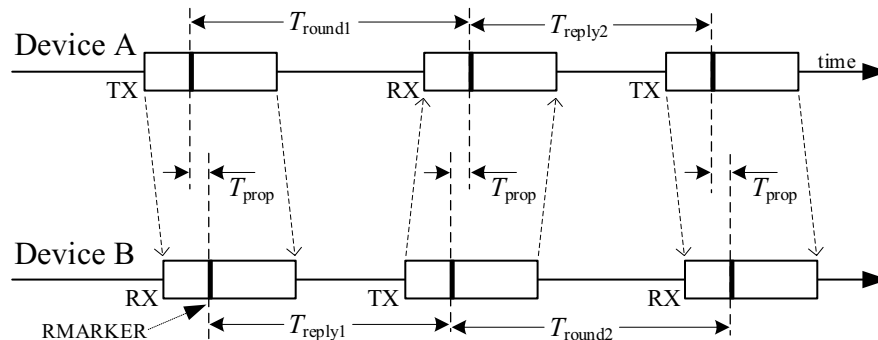


Figure 6-47c—DS-TWR with three messages

6.9.1.2.5 Time difference of arrival (TDOA)

TDOA is a technique to locate a mobile device, (e.g., a radio frequency identification (RFID) device), based on the relative arrival times of a single message or multiple messages. OWR is used for TDOA. There are two cases of TDOA. In one case a message is periodically broadcast by the mobile device to multiple fixed nodes that are synchronized in some way so that the arrival times can be compared. Typically, the message sent by the mobile device is referred to as a blink. In the other case, multiple synchronized nodes broadcast messages sequentially with known transmission time offsets with respect to each other. For any pair of fixed synchronized nodes, the difference in arrival time of the blink in the first case, or the broadcast messages at the mobile device in the second case, places the mobile device on a hyperbolic surface. Combining the results from multiple such pairs will yield an intersection point between the sets of hyperbolic surfaces yielding the location of the mobile device. Note that in the second case, the transmission offset is taken into account when calculating the difference in arrival time of messages from synchronized nodes.

RFID devices typically use the shortest blink message possible, (e.g., a multipurpose frame) to reduce power consumption. A multipurpose frame can be as short as 12 octets; consisting of a Short Frame Control field, the Sequence Number field, no destination address field, an extended source address and an FCS.

Synchronization of fixed nodes can be achieved by a wired distribution of the clock signals. However wireless synchronization schemes are also practical. These may use UWB messages sent between the fixed nodes (and a known/pre-measured TOF) to calculate the relative clock frequency offset and drift between the fixed nodes and use this information to correct the arrival times of the blink messages into a common timebase for the TDOA data to be meaningful.

6.9.1.3 Ranging counter

The ranging counter supported by an RDEV is a set of behavioral properties and capabilities of the RDEV that produce ranging counter values. A ranging counter value is an unsigned integer of, at minimum, 32-bit length. The unit of this counter is specified in 6.9.1.4.

6.9.1.4 Ranging counter time unit

The time unit of the ranging counter as used in MCPS-DATA primitives and ranging time related IE differs depending on the PHY.

- For the HRP UWB PHY the time unit is 2^{-7} of the 499.2 MHz chipping period, which is approximately 15.65 ps.
- For the LRP UWB PHY the time unit is 2^{-20} of the basic chipping rate of 1 MHz, which is approximately 0.9537 ps.
- For the TVWS PHY the time unit is 10 ps.

The next higher layer is responsible for the TOF calculations and interpreting the time unit of the ranging counter correctly depending on the current PHY.

6.9.1.5 Ranging scheduling time unit

The ranging scheduling time unit (RSTU) applies in the MAC for specifying ranging slot durations and various time intervals for scheduling of ranging activities. The RSTU value depends on the current PHY as specified in Table 6-4a.

Table 6-4a—PHY dependent RSTU values

PHY	RSTU
HRP UWB PHY	416 chips = $416 \div (499.2 \times 10^6) \approx 833.33$ ns
LRP UWB PHY	1 μ s = 1 chip at 1 MHz basic chipping rate

The ERDEV MAC shall maintain a 24-bit RSTU time counter relative to which slot timings and associated packet transmissions and receive enables are referenced.

6.9.1.6 Crystal characterization

6.9.1.6.1 Crystal characterization overview

An RDEV that implements optional crystal characterization shall produce a tracking offset value and a tracking interval value for every ranging report. The tracking offset and the tracking interval are computed from measurements taken during an interval that includes the interval bounded by the ranging counter start value and the ranging counter stop value. Note that crystal characterization is relevant only if it is characterizing the crystal that affects the ranging counter.

6.9.1.6.2 Ranging tracking offset

The ranging tracking offset provides information on the difference between the transmitter and receiver reference oscillator frequencies. The value is a signed integer, which shall be positive when the oscillator at the transmitter operates at a higher frequency than the oscillator at the receiver, and negative when the

oscillator at the transmitter operates at a lower frequency than the oscillator at the receiver. The value represents the difference in frequency between the receiver's oscillator and the transmitter's oscillator after the tracking offset integer is divided by the ranging tracking interval integer of 6.9.1.6.3. The precision shall be at least 19 bits.

6.9.1.6.3 Ranging tracking interval

The ranging tracking interval is an unsigned integer value that represents the duration in a message exchange over which the tracking offset was measured. The size of the ranging tracking interval should be chosen to allow reporting (in conjunction with the ranging tracking offset value defined in 6.9.1.6.2) of crystal offset values down to 100 parts per billion, or better. Greater precision is encouraged, as described in "Applications of IEEE Std 802.15.4" [B3].

6.9.1.7 Ranging FoM

An RDEV shall produce a Ranging FoM for every ranging counter value that is produced. The Ranging FoM shall be formatted as shown in Figure 6-47d.

Bits: 0–2	3–4	5–6	7
Confidence Level	Confidence Interval	Confidence Interval Scaling Factor	Extension

Figure 6-47d—Ranging FoM

The Confidence Level field conveys the probability that the RMARKER arrived during the Confidence Interval, as specified in Table 6-4b.

The Confidence Interval field specifies the confidence interval as defined in Table 6-4c. The duration of the Confidence Interval in Table 6-4c is the duration of the entire interval, not a plus or minus number.

The Confidence Interval Scaling Factor field is defined in Table 6-4d.

The overall confidence interval is obtained according to the formula:

$$\text{Overall confidence interval} = \text{Confidence Interval} \times \text{Confidence Interval Scaling Factor}.$$

When the Extension field is zero, the fields have the meanings given in Table 6-4b, Table 6-4c, and Table 6-4d.

Table 6-4b—Confidence Level field

Confidence Level field value	Confidence level
0	No FoM
1	20%
2	55%
3	75%
4	85%

Table 6-4b—Confidence Level field (*continued*)

Confidence Level field value	Confidence level
5	92%
6	97%
7	99%

Table 6-4c—Confidence Interval field

Confidence Interval field value	Confidence interval
0	100 ps
1	300 ps
2	1 ns
3	3 ns

Table 6-4d—Confidence Interval Scaling Factor field

Confidence Interval Scaling Factor field value	Confidence interval scaling factor
0	0.5
1	1.0
2	2.0
3	4.0

The FoM characterizes the accuracy of the PHY estimate of the arrival time of the RMARKER at the antenna. The FoM shall characterize the accuracy of the timer counter value in the same report primitive.

When the Extension field is set to one, the Ranging FoM shall be formatted as shown in Figure 6-47e.

Bits: 0–6	7
Extension Value	Extension = 1

Figure 6-47e—Ranging FoM format when the Extension field is one

The FoM value having its Extension field set to one and Extension Value field set to zero is specifically used to signal to the next higher layer that the RxRangingCounter value is not correct and the higher layer should use the sounding primitives, for example MLME-SOUNDING.request, see 8.2.16, to retrieve the channel sounding information and use it to determine the ranging counter value to ascribe to the received packet. All other Extension Value field values are reserved.

6.9.2 Set-up activities before a ranging exchange

Change 6.9.2 as follows:

The mandatory part of ranging is limited to the generation of transmit and receive ranging counter time timestamp reports during the period that ranging is enabled in an RDEV. It is possible that an RDEV will consume more power when ranging is enabled; therefore, a natural default for an application would be to have ranging disabled. The higher layer is responsible for enabling ranging in both RDEVs involved in a TWR exchange. Prior to a two-way ranging exchange, both RDEVs involved in the exchange shall already have ranging enabled. Furthermore, if the optional dynamic preamble selection (DPS) capability is to be used, it is assumed there has been some sort of coordination of the preamble and channel selection preambles prior to the TWR two-way ranging exchange. How this coordination and enabling actually is accomplished is up to the implementer, beyond the scope of this standard. It may be perfectly acceptable to accomplish the coordination and enabling with a clock and a look-up table that says what a device should do at a particular time. Because coordination generally involves communication and because the PHYs are designed to achieve communication, it is natural to suggest that the PHY be used for coordination. The Ranging Channel and Preamble Code Selection IE (RCPCS IE), as specified in 7.4.4.48, can be included in a frame exchange prior to the ranging exchange, or out-of-band signaling, as well as custom messages, may be used for this coordination.

6.9.3 Finish-up activities after a ranging exchange

Change 6.9.3 as follows:

At the end of a two-way exchange, each device is in possession of TX and RX ranging counter values giving the round-trip time measurement or reply time as appropriate a timestamp report. To compute the TOF accomplish anything useful, both of these values are needed those timestamp reports shall eventually come to be at the same node where the computations are performed. How this movement of these values timestamp reports is accomplished is beyond the scope of this standard up to the implementer. Timestamp reports are just data. Because movement of data involves communication and because the PHYs are designed to achieve communication, it is natural to suggest that the PHY be used for the final consolidation of timestamp reports. Out-of-band signaling as well as custom messages or the Ranging Measurement Information IE (RMI IE), as specified in 7.4.4.46, can be used for this purpose as described in 6.9.6.3.

The application is responsible for enabling the ranging mode in the RDEV before a ranging exchange. After a ranging exchange, the application is again responsible for disabling the ranging mode in the RDEV. If the application fails to disable the ranging mode in the RDEV, there will be no algorithmic harm. Ranging mode is fully compatible with other uses of the RDEV, and the only result of leaving ranging enabled when it is not really being used is that the RDEV will generate useless timestamp reports while potentially consuming more power. #

Change the title of 6.9.4 as follows:

6.9.4 Managing DPS and DCS

Insert a new subclause heading 6.9.4.1 to contain the existing text and figure from 6.9.4 as follows:

6.9.4.1 Managing DPS

Change the first paragraph of 6.9.4 (now 6.9.4.1) as follows:

Figure 6-48 shows a suggested message sequence for TWR two-way ranging. The messages represented in the two top dotted boxes are simply suggestions showing how the communications capability of the RDEV can be used to accomplish the ranging setup activities. The messages in the bottom dotted box are

suggestions showing how the communications capability of the RDEV can be used to accomplish the ranging finish-up activities.

Replace Figure 6-48 with a new figure as follows:

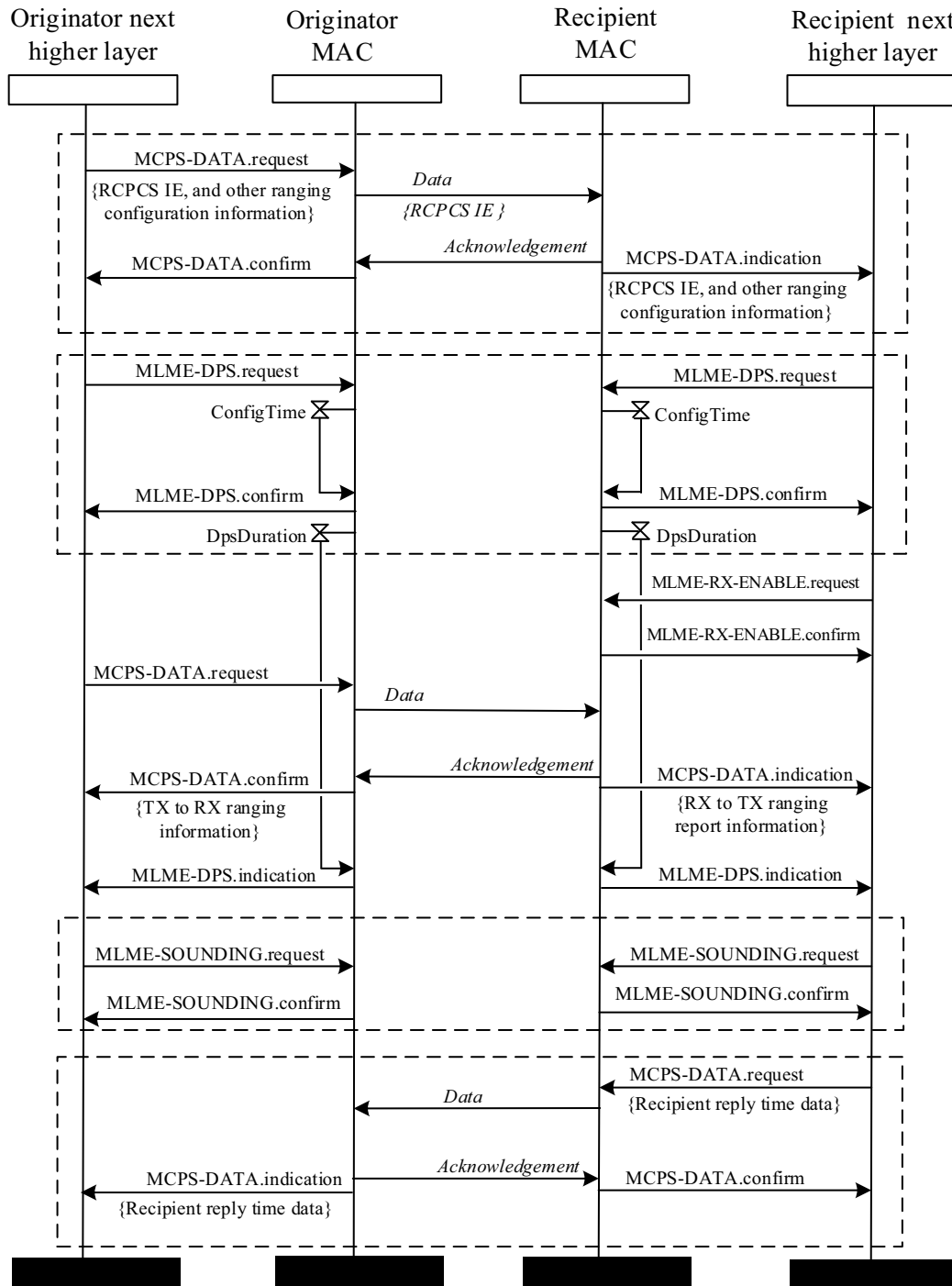


Figure 6-48—A message sequence for ranging

Change paragraphs two and three of 6.9.4 (now 6.9.4.1) as follows:

The top dotted box in Figure 6-48 illustrates the use of a data exchange to effect the coordination of the preamble codes and channel preambles to be used for a TWR two-way ranging exchange. The coordination of preambles is needed only when using the optional DPS capability of the PHY. As illustrated in Figure 6-48, for the ERDEV, the choice of preamble code and channel number can be exchanged using the RCPCS IE (described in 7.4.4.48). If optional DPS is not used, the communication sequence in the top box can be thought of as arranging for the recipient RDEV to become aware that a ranging exchange is desired and that the recipient next higher layer should enable ranging in the recipient PHY. The ranging procedures in 6.9.6 and 6.9.7 describe mechanisms provided by this standard through which this can be achieved. The second from the top dotted box in Figure 6-48 illustrates the use of the MLME-DPS.request, as described in 8.2.15.2, and the MLME-DPS.confirm, as described in 8.2.15.3. Use of these primitives is unique to the optional DPS mode of ranging.

The next higher layer of the ERDEV can optionally specify a future time at which to apply the preamble code and/or channel number using the ConfigTime parameter of the MLME-DPS.request. The time at which to make the DPS change can be exchanged via the CCI field of the RCPCS IE. It is the responsibility of the next higher layer to ensure that the channel selection reflects the regional regulation. If the selected channel is not supported by the device, the DPS will fail, and the MLME-DPS.confirm primitive shall report a Status parameter value of NOT_SUPPORTED.

Upon the assertion of the MLME-DPS.confirm primitives, as illustrated in Figure 6-48, both of the devices PHYs have switched to use the alternative from the normal length preamble symbols to long preamble symbols and/or channel number as selected by the MLME-DPS.request. This is desirable behavior intended to help hide the PHYs' transmissions from other malicious nodes in the network and protect the devices PHYs from transmissions by other malicious nodes in the network. A side effect of this mode is that neither device PHYs can communicate with the rest of the network. To prevent the devices from losing connectivity PHYs from becoming lost as a result of this optional behavior, the MAC sublayers on both sides of the link shall initiate timers after issuing the MLME-DPS.confirm with Status of SUCCESS sending the frame (for the originator) or receiving the frame (for the recipient). If the timer duration is exceeded before the MAC sublayer issues receives the MCPS-DATA.confirmeconfirm (for the originator) or the MCPS-DATA.indication primitive (for the recipient), then the MAC sublayer shall initiate a MLME-DPS.indication to the next higher layer as described in 8.2.15.4. Not shown in Figure 6-48, one responsibility of the application, if the optional DPS capability is used, is to initiate the MLME-DPS.request primitive on both sides of the ranging link at the completion of the ranging exchange. Most typically, this MLME-DPS.request primitive would be part of the finish-up activities and would have both TxDpsIndex and RxDpsIndex set to zero to return the PHYs to using the phyCurrentCode and phyCurrentChannel from the PIB. Also not shown in Figure 6-48, another responsibility of the application is to initiate a MLME-DPS.request primitive in response to an MLME-DPS.indication. Most typically, this MLME-DPS.request primitive would have both TxDpsIndex and RxDpsIndex set to zero and return the PHY to using phyCurrentCode from the PIB.

Change the title and text of 6.9.5 as follows:

6.9.5 The basic ranging exchange

This subclause describes the basic ranging exchange. Enhanced ranging procedures that employ IEs for their control and for ranging information exchange are described in 6.9.6 and 6.9.7. These subclauses include message sequence charts to illustrate the procedures. The use and support of any of these ranging procedures and associated IEs is optional.

The essential core of the ranging exchange is shown in Figure 6-48 starting just after below the MLME-DPS exchange. The application is responsible for initiating the MLME-RX-ENABLE.request primitive, as described in 8.2.10.2, with RangingControl RangingRxControl equal to RANGING_ON. Once the RDEV

has received the MLME-RX-ENABLE.request primitive with RangingControl ~~RangingRxControl~~ equal to RANGING_ON, all future RFRAMES received by the RDEV shall generate TX and RX ranging counter timestamp reports until ranging is disabled.

At the initiator, the application is responsible for initiating a MCPS-DATA.request primitive with Ranging and RangingPhr values (in the DataRequestRangingDescriptor parameter) both set to TRUE ~~equal to ALL_RANGING~~. Upon receipt of a MCPS-DATA.request primitive with Ranging equal to TRUE ~~ALL_RANGING~~, RDEV shall generate ranging timestamp reports for all RFRAMES after the transmit frame is transmitted. The ranging timestamp reports will continue until ranging is disabled. The TX-to-RX turnaround enabling the originator to receive the Ack frame is necessary and is not shown in Figure 6-48. This turnaround is the normal turnaround that is done for any exchange expecting an acknowledgment. The turnaround happens without any action required by the originator next higher layer. Ranging Timestamp reports are generated and passed to the next higher layer independent of the state of the AR field in the MAC header of received RFRAMES.

As shown in Figure 6-48, the first ranging timestamp report to the originator next higher layer is via parameters shall come back as elements of the MCPS-DATA.confirm primitive. The first ranging timestamp report to the recipient next higher layer is via parameters shall come back as elements of the MCPS-DATA.indication primitive. All subsequent ranging timestamp reports on either side of the link are via parameters shall come back as elements of MCPS-DATA.indication and MCPS-DATA.confirm primitives. The potential additional MCPS-DATA.indication primitives that may would be due to unexpected stray RFRAMES are not shown in Figure 6-48 for simplicity. The timestamp reports due to any strays shall continue until ranging is disabled. The generation of ranging reports reporting of timestamps for a stream of stray RFRAMES "strays" is the behavior that enables the RDEV to be used as an infrastructure RDEV RDEVs in OWR one way ranging applications. OWR One way ranging is described in "Applications of IEEE Std 802.15.4" [B3].

For non-TVWS RDEVs, the timestamp is defined in ~~15.7~~ 6.9.1.1. Use of nonzero TX and RX ranging counter timestamp reports is limited to RDEVs. Only devices that have *phyRanging* set to TRUE shall return a ranging nonzero timestamp report to a next higher layer.

For TVWS RDEVs, the Timestamp IE, 7.4.4.26, and the Timestamp Difference IE, 7.4.4.27, are provided for exchanging timing information between TVWS RDEVs to support the ranging feature.

For information on the use of the MLME-SOUNDING primitives see section 7.1.1.4.5 of "Applications of IEEE Std 802.15.4" [B3].

Insert new subclauses 6.9.6 to 6.9.11 after 6.9.5 as follows:

6.9.6 Ranging procedures

6.9.6.1 General ranging procedures

The layers above the MAC are responsible for the decision to participate in a TWR exchange between a pair of devices and for the final calculation of the resulting range. Ranging procedures appropriate to the ranging methods described in 6.9.1.2 are defined in 6.9.6, 6.9.7, and 6.9.8. The use and support of any of these ranging procedures and associated IEs is optional.

Irrespective of whether the ranging reports are coming from an RDEV or an ERDEV, the same procedures apply, (i.e., any reference to RDEVs also applies to ERDEVs). However, an ERDEV provides additional primitives, based on which the higher layer can modify the action it takes (e.g., replying in a ranging exchange, or considering the ranging result as good) depending on its validation of the timestamp result. For example, in the case of the HRP-ERDEV this may be done using the *RangingStsS1Fom* parameter(s) of the MCPS-DATA.indication primitive.

6.9.6.2 Control of ranging and the transfer of results

Information elements can be employed to control TWR and the transfer of ranging data between the RDEVs participating in the ranging exchange. With reference to the ranging methods defined in 6.9.1.2.2 and 6.9.1.2.3, to complete the calculation of the TOF between two RDEVs participating in a ranging exchange, depending on the use case it is necessary to combine measurements made by both devices. That is, one device will need to transfer its ranging measurements to the other. Information elements are specified to provide a mechanism to control TWR and support the transfer of ranging information between the devices participating in the ranging exchange. To ensure the integrity of this information transfer it is recommended to employ the secure private data communication capability of this standard.

6.9.6.3 Ranging procedure for SS-TWR with deferred reply time result

For an SS-TWR with a deferred reply time result, the ranging exchange is initiated by the next higher layer invoking the MCPS-DATA.request primitive to send a ranging frame including the Ranging Request Measurement and Control IE (RRMC IE), described in 7.4.4.45, requesting the ranging reply time information, and with Ranging Control Information field set according to Table 7-52k.

The replying ranging frame completes the round-trip time measurement and the MCPS-DATA.confirm primitive gives the initiating side a ranging report that defines the round-trip time. At the responding side, the MCPS-DATA.indication primitive supplies the responding side ranging report that defines the reply time for the round-trip time measurement. This reply time is communicated to the initiating side in the RMI IE (described in 7.4.4.46), carried by a subsequent message.

Figure 6-48a shows the message sequence chart for this exchange, where RRMC IE (0) indicates an RRMC IE with the Ranging Control Information field value of zero. When the initiator next higher layer receives the RMI IE it has sufficient information to calculate the TOF between the two devices using one of the formulas given in 6.9.1.2.2.

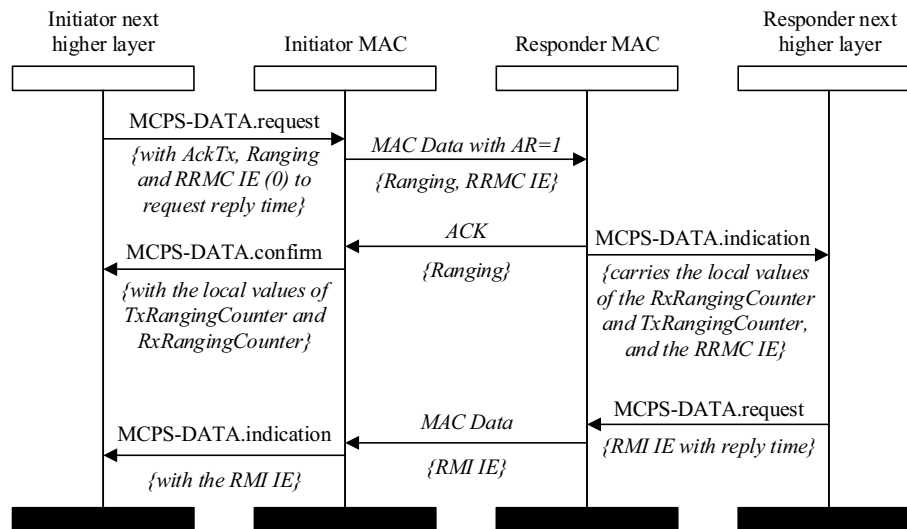


Figure 6-48a—Message sequence chart for SS-TWR with deferred reply time result

6.9.6.4 Ranging procedure for SS-TWR with embedded reply time result

For an SS-TWR with an embedded reply time result, the ranging exchange is initiated by a ranging frame including the RRMCI IE (described in 7.4.4.45) requesting the ranging reply time information, and with the Ranging Control Information field set according to Table 7-52k. The responding device completes the round-trip measurement by sending a reply frame with an embedded Ranging Reply Time Instantaneous IE (RRTI IE) as specified in 7.4.4.35. When a device is capable of generating an RRTI IE, it can minimize the number of messages needed for a ranging measurement and thus save power, see Figure 6-47a and its associated description in 6.9.1.2.2 for details. However, it takes time to calculate the arrival time of the received ranging message and prepare the RRTI IE value. While in some cases this time may be known a priori by an out-of-band means, the Ranging Reply Time Negotiation IE (RRTN IE) as specified in 7.4.4.49 provides a mechanism for such a device to indicate its preferred reply time, that is how long it needs to prepare the frame with the RRTI IE. When this time is known, the ranging initiating device can expect the response message after the specified time and can save energy by delaying turning on the receiver until then. This is applicable in both SS-TWR and DS-TWR ranging exchanges.

Figure 6-48b shows the message sequence chart for this exchange, where RRMCI IE (0) indicates an RRMCI IE with the Ranging Control Information field value of zero. The communication of the RRTN IE, shown in the dashed box, may happen at any convenient time before the ranging exchange is initiated, or the preferred reply time information may be pre-known or exchanged out-of-band. Upon receipt of the MCPS-DATA.indication primitive conveying the responder's RRTI IE, the initiator next higher layer has sufficient information to calculate the TOF between the two devices according to one of the formulas given in 6.9.1.2.2.

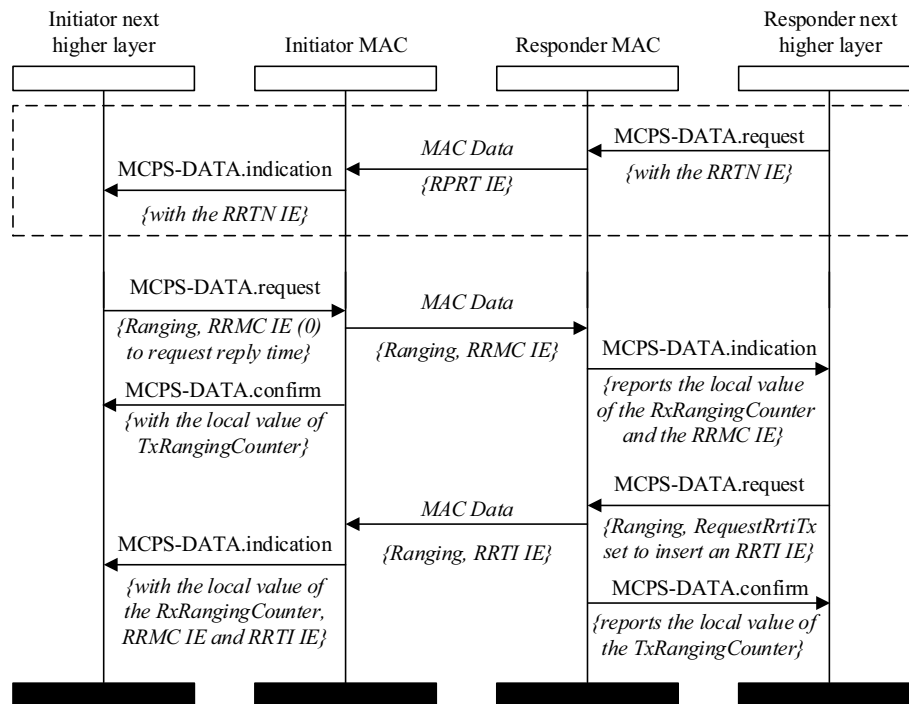


Figure 6-48b—Message sequence chart for SS-TWR with embedded reply time

6.9.6.5 Ranging procedure for SS-TWR with fixed reply time

Where a responding device has precise control of the transmit time of its response message with respect to the arrival time of the ranging initiation message, then the reply time, T_{reply} in Figure 6-47a, may be a fixed known quantity, agreed between the parties participating in the ranging exchange. In this case it is not required to embed T_{reply} into the response message or to send it separately in an additional message. The accuracy of the resultant range will depend on how fine a control the responding device has on the transmit time of its response message, where every 1 ns error in TOF translates to approximately 30 cm range error.

The HRP-ERDEV PPDU format SP3 might be employed in the case of fixed reply time. Figure 6-48c shows an example message sequence chart for such a ranging exchange.

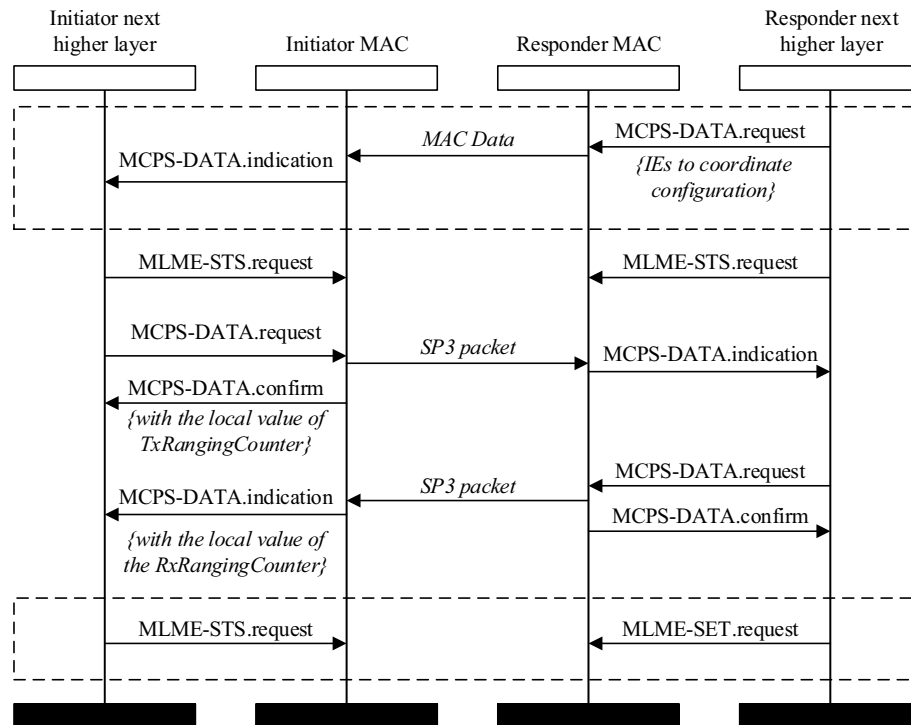


Figure 6-48c—Message sequence chart for SS-TWR using SP3 packets

The initial message in the dashed box represents the communication between devices to coordinate and agree on the use of SP3 packets and on all other necessary parameters to allow the communication to proceed. While only a single message is shown in the figure, there may be a series of messages in each direction to agree on all the parameters. For example, the RRTN IE (described in 7.4.4.49) can be used to agree on the fixed reply time.

The next higher layer is responsible for properly configuring the operation at each end using the MLME-STS.request primitive to configure the SP3 packet format at both ends, and for setting the PIB attributes *phyHrpUwbStsKey*, *phyHrpUwbStsVCounter*, and *phyHrpUwbStsVUpper96* to the correct values. Once the higher layer has selected the SP3 packet configuration, subsequent MCPS-DATA primitives relate to SP3 packets, until the higher layer uses the MLME-STS.request primitive to change the packet configuration.

The MCPS-DATA.request primitive is used to initiate the ranging exchange, even though in this mode the PPDU does not convey MAC data. Not shown, but assumed, is the invoking of the MLME-RX-ENABLE.request primitive to turn on the receiver at the appropriate time to receive the PPDU. Since the

PHY is configured for SP3 packets, the PHY indicates reception of the PPDU to the MAC layer at the end of the STS and the MAC, similarly aware of the SP3 configuration, delivers the RxRangingCounter value in the RangingReportDescriptor parameter of the MCPS-DATA.indication primitive. Also, assuming the RangingStsFom in the RangingReportDescriptor is acceptable, the higher layer may initiate the response by invoking an MCPS-DATA.request primitive specifying a RangingTxTime in line with the agreed fixed reply time.

When the SP3 packet response is received at the initiating device, and again assuming that the RangingStsFom in the RangingReportDescriptor parameter of that MCPS-DATA.indication primitive is acceptable, the initiating end has sufficient information, given the known fixed reply time, to calculate the TOF between the two devices according to one of the formulas given in 6.9.1.2.2.

The ranging exchanges are repeated as many times as the higher layers have mutually agreed. To resume PHY and MAC data interactions, the next higher layer uses the MLME-STX.request primitive to restore the STS packet configuration to a value that allows such data interactions. This is shown in the final dashed box in Figure 6-48c.

The LRP-ERDEV also supports challenge-response ranging with fixed reply time, to remove the need for a data message to convey the reply time. The procedures for this are defined in 6.9.8.4.

6.9.6.6 Ranging procedure for DS-TWR with deferred reply time information

DS-TWR essentially involves completing SS-TWR exchanges initiated at either end and combining the results. The DS-TWR exchange is initiated by the next higher layer sending a ranging data frame carrying an RRMC IE (described in 7.4.4.45) with the Ranging Control Information field set according to Table 7-52k. This frame and its acknowledgment define the first round-trip time measurement, while the RRMC IE delivery in the MCPS-DATA.indication primitive tells the next higher layer to initiate the second round-trip time measurement of the exchange by the sending of a Data frame in the other direction. This Data frame includes an RRMC IE with the Ranging Control Information field set according to Table 7-52k to indicate this is the continuation of the exchange and both of the Reply Time Request and Round-trip Time Request fields set to one to request the reply time and the result of the first round-trip time measurement. The acknowledgment to this message completes the second round-trip time measurement. A subsequent message from the initiator conveys the first round-trip time measurement and the reply time for the second round-trip time measurement in an RMI IE (described in 7.4.4.46). Figure 6-48d shows the message sequence chart for this exchange. In the figure the designation RRMC IE (2) means an RRMC IE with its Ranging Control Information field set to two, and designation RRMC IE (3) means an RRMC IE with its Ranging Control Information field set to three. When the responder receives the second MCPS-DATA.indication primitive (with the RMI IE), it has sufficient information to calculate the TOF between the two devices according to the formula given in 6.9.1.2.3. The subsequent reporting of the ranging result to the initiating end, using the RMI IE, depends on the value of the TOF Request field in the initiating RRMC IE.

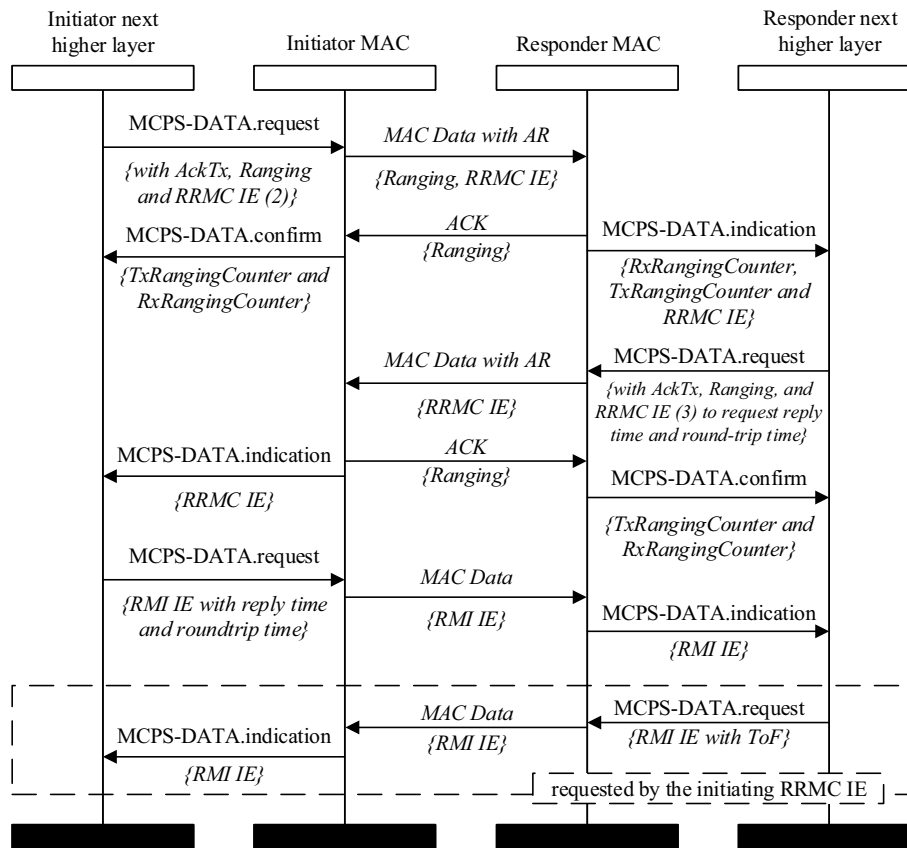


Figure 6-48d—Message sequence chart for DS-TWR with deferred reply time result

6.9.6.7 Ranging procedure for DS-TWR with embedded ranging time information

To achieve the three-message DS-TWR exchange described in Figure 6-47c requires that the initiating end is able to embed the reply time as part of completing the second round-trip time measurement. With reference to the message sequence chart of Figure 6-48e, the DS-TWR is initiated by an RFRAME carrying an RRMC IE (described in 7.4.4.45) with its Ranging Control Information field set according to Table 7-52k, and TOF Request field set to zero indicating that the initiating end does not require a report of the ranging. In the figure, the designation RRMC IE (2) means an RRMC IE with its Ranging Control Information field set to two, and designation RRMC IE (3) means an RRMC IE with its Ranging Control Information field set to three.

The responding side completes the first round-trip time measurement and initiates the second measurement with an RFRAME carrying an RRMIC IE with control field set according to Table 7-52k to indicate this is the continuation of the exchange and with the Reply Time Request field and Round-trip Time Request field both set to one, indicating requests for the first round-trip time measurement and the reply time for the second round-trip time measurement. The initiator completes the exchange by sending a final RFRAME carrying the first round-trip time measurement in an RMI IE (described in 7.4.4.46) and the reply time of this second round-trip time measurement in an RRTI IE (as described in 7.4.4.35).

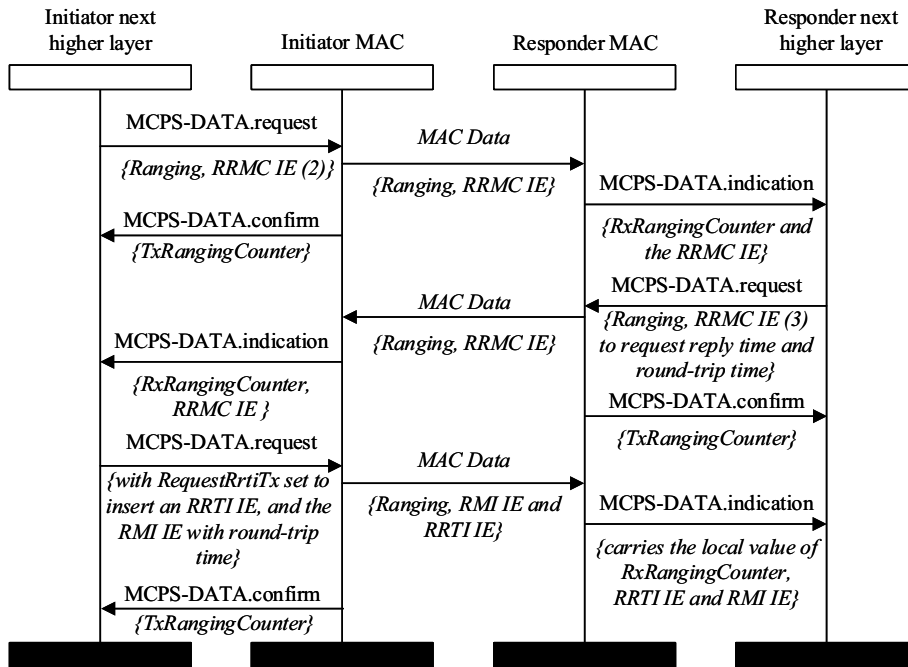


Figure 6-48e—Message sequence chart for DS-TWR with three messages

When the responder higher layer receives the second MCPS-DATA.indication primitive, it has sufficient information to calculate the TOF between the two devices according to the formula given in 6.9.1.2.3. When the initiator of the ranging exchange wants the result, it will set the TOF Request field of the initiating RRM IE, to ask the responding end to convey the result in an RMI IE in a subsequent message at the end of the exchange as shown in Figure 6-48d.

6.9.6.8 Other procedures for coordinating RDEV and ERDEV

For successful interworking of HRP-ERDEV when an STS is being employed, the transmitter and receiver need to be aligned with respect to the seed (i.e., STS key and data value V) used in the transmitter to generate the STS and used in the receiver to generate the sequence to correlate with the received STS. To coordinate these values, the secure private data communication capability of this standard may be used to transfer the seed between devices using the Ranging STS Key and Data IE (RSKD IE) as described in 7.4.4.42. The counter value within the RSKD IE can relate to the current packet or a future one, as is indicated by the CP field of the IE. The higher layer is responsible for using the received RSKD IE information to configure the STS seed, (via *phyHrpUwbStsKey*, *phyHrpUwbStsVUpper96*, and *phyHrpUwbStsVCounter* PIB attributes), appropriately for its future packet transmissions and receptions. A header IE version of the RSKD IE is also defined, in 7.4.2.20, to facilitate synchronization of STS generators using information sent in the clear while accompanied by secured payload IEs and data.

When receiving a received frame that contains an RSKD IE header IE, it is intended that the IE is delivered to the next higher layer to allow it to set the *phyHrpUwbStsKey*, *phyHrpUwbStsVUpper96*, and *phyHrpUwbStsVCounter* attributes appropriately for STS generation. If a frame containing an RSKD IE header IE fails to pass the incoming security processing, for example if the receiver does not have the key to validate the MIC, the RSKD IE shall be delivered to the next higher layer via the HeaderIEList parameter of the MLME-COMM-STATUS.indication.

Similarly, when using DPS as described in 6.9.4, the RDEVs need to coordinate the preamble codes and channel selection they are going to employ and again the secure private data communication capability of this standard can be used to transfer the selected preamble code indices and channel number values between devices using the RCPCS IE (as described in 7.4.4.48).

6.9.6.9 Secure transactions

The enhanced ranging capabilities of the ERDEV can be used to protect transactions by using ranging to check that the distance between the communicating devices is as expected. In such secure service transaction scenarios, the higher layer is often interfacing between the radio and a secure element used in validating the transaction. When used for this purpose, the MPX IE shall be used as follows: (refer to Figure 9 of IEEE Std 802.15.9). The Transaction Control field consists of a 3-bit Transfer Type field and a 5-bit Transaction ID field.

The Transfer Type field shall be set to one (0b001) to indicate that the Multiplex ID associated with the dispatch code for the MPX IE is indicated by the Transaction ID field of the Transaction Control field. The Transaction ID field contains the five least significant bits of the Multiplex ID used as the dispatch code as defined in Table 20, of IEEE Std 802.15.9, and is used as an identifier to specify that this frame contains information used for Ranging Enhanced Secure Transactions.

The MPX IE with the dispatch code 0x0010, (16 decimal), for Ranging Enhanced Secure Service Transactions, is applicable to higher layer protocols that support transactions with a secure component in the device. When an MPX IE with the Transaction ID for Ranging Enhanced Secure Service Transactions is received in an RFRAME, the MAC delivers it to the higher layer with an associated ranging measurement, which the higher layer can use to limit access based on range. When used for this purpose, the Upper-Layer Frame Fragment field of the MPX IE carries information to identify and distinguish transactions, with MAC payload used by the next higher layer to route the payload, and shall be formatted as shown in Figure 6-48f. This information can be used by the respective device components (e.g., a secure element) to select the appropriate STS used for ranging. If a transaction takes place using multiple frames, all frames that transport data belonging to this particular transaction should include the MPX IE with the same Transaction ID and USSID value.

Bits: 0–2	3–5	6–10	11–15	Octets: variable	variable
Payload Type	Reserved	USSID Length	Additional Info Length	USSID	Additional Info

Figure 6-48f—Format of Upper-Layer Frame Fragment field of MPX IE for Ranging Enhanced Secure Service Transactions

The Payload Type field specifies the type of the content contained in the MAC Payload field. The Payload Type field shall have one of the non-reserved values defined in Table 6-4e.

The USSID Length field specifies the number of octets in the USSID field. The valid range for USSID Length shall be 0 to 16.

Table 6-4e—Values of Payload Type field

Payload Type field value	Meaning
0	Application specific payload.
1	MAC Payload field contains an APDU as defined by ISO/IEC 7816-4.
2	MAC Payload field contains a Mifare Classic® command or response.
3	MAC Payload field contains a Mifare Desfire® command or response.
4	MAC Payload field contains an Information field as defined by JIS X 6319-4.
5–7	Reserved.

The USSID field is used to identify and distinguish transactions. All frames that transport data belonging to the same transaction should use the same USSID value. The content of the USSID field depends on the Payload Type as per Table 6-4f. It is impossible to support differentiation of transactions with the same Payload Type value unless a USSID is provided. The USSID field includes an ID that identifies the target application for the transaction.

Table 6-4f—Permissible USSID depending on Payload Type field in Secure Service IE

Payload Type field value	Permissible content of the USSID Length and USSID fields
0	Either the USSID field contains an application specific payload info or the USSID Length field is set to zero.
1	Either the USSID field contains an application identifier (AID) formatted as specified in Figure 6-48g or the USSID Length field is set to zero, in which case the transaction is assumed to use implicit selection as defined in ISO/IEC 7816-4.
2	USSID Length field is set to zero.
3	Either the USSID field contains an AID formatted as specified in Figure 6-48g or the USSID Length field is set to zero.
4	The USSID Length field is set to two and the USSID field contains a system code (SC) formatted as specified in Figure 6-48h.

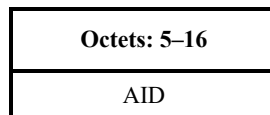


Figure 6-48g—Format of USSID field when carrying an AID

The AID is an Application Identifier as defined in ISO/IEC 7816-5.

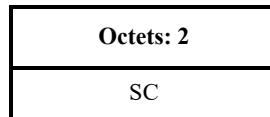


Figure 6-48h—Format of USSID field when carrying an SC

The SC is a system code as defined by JIS X 6319-4.

The Additional Info Length field is an unsigned integer that specifies the number of octets in the Additional Info field.

The Additional Info field is used to provide a summary of the transaction, which can be used for user information and authorization. If present, the Additional Info field contains a string that can be used to provide additional information to the higher layer about the transaction to be performed. The encoding of characters into the Additional Info field follows UTF-8 [B7b]. Line breaks in the string are represented using a carriage return (CR) followed by a line-feed (LF), that is 0x0D, 0x0A in UTF-8. The Additional Info field should be present in the first frame used by a transaction.

6.9.7 Multi-node ranging

6.9.7.1 Introduction

The use and support of the procedures and associated IEs in this subclause are optional. An RCM is a data frame conveying the Advanced Ranging Control IE (ARC IE) described in 7.4.4.36. The RCM can be used to convey ranging parameters to control and configure aspects of the ranging procedure(s) such as the time-slot structure shown in Figure 6-48j, the ranging methods specified in 6.9.1.2, and the STS packet configuration as specified in 15.2.

The following nomenclature is used for ERDEVs:

- Controller: An ERDEV that controls the ranging and defines the ranging parameters by sending an RCM.
- Controlee: An ERDEV that utilizes the ranging parameters received from the controller in the RCM.
- Initiator: An ERDEV that following the RCM, initiates a ranging exchange by sending the first message of the exchange, the ranging initiation message. A controller or a controlee can be an initiator.
- Responder: An ERDEV that responds to the ranging initiation message received from the initiator.

These terms are illustrated in Figure 6-48i.

The next higher layer of the controller is responsible for determining the ranging parameters and the role of the participating ERDEVs as either initiators or responders. Unless it is otherwise specified that the MAC is acting, the terms controller and controlee refer to those entities' next higher layer being informed of the event or taking the action being described.

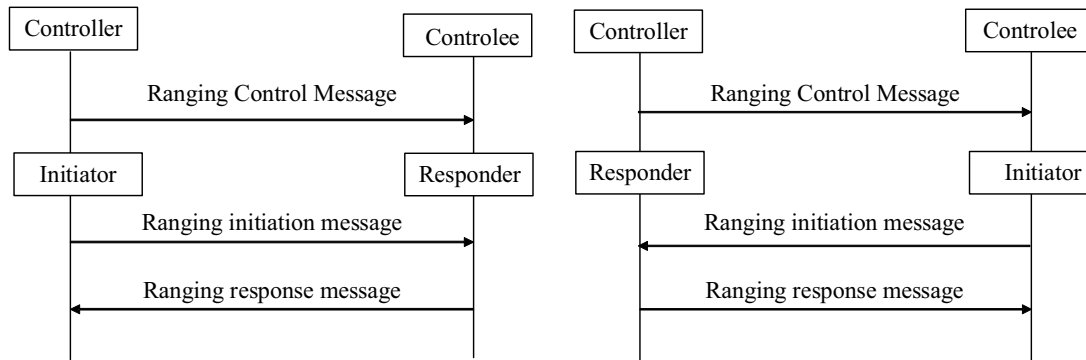


Figure 6-48i—Ranging controller, controlee, initiator, and responder

Multi-node ranging is a ranging procedure in which one or more initiators perform ranging with a number of responders. There are two types of multi-node ranging, as indicated by the Schedule Mode field of the ARC IE defined in 7.4.4.36. The first type is time-scheduled ranging in which the controller knows the identities of all controlees and specifies the precise schedule of ranging transmissions. The second type is contention-based ranging in which the controller may not know the number or identities of the controlees, and hence the ERDEVs contend with each other. Note that in the case of contention-based ranging, collision between responding devices is possible; the upper layer is responsible for filtering out inaccurate or wrong ranging results.

For time-scheduled ranging, the controller uses the Ranging Device Management IE (RDM IE) defined in 7.4.4.44 to select the participating ranging devices, specify their role as either initiator or responder, and assign their time slots. The RDM IE can be omitted from the RDM in the case where the roles and transmission schedule is pre-determined or conveyed via some out-of-band mechanism.

For contention-based ranging, the ERDEVs, that is initiator or responder devices, contend to transmit in the appropriate time slots. The Ranging Contention Phase Structure IE (RCPS IE), defined in 7.4.4.40, is used to specify different phases (see 6.9.7.2) for initiators and responders to contend, which can be conveyed in the RCM (in addition to the ARC IE). To ensure the relative fairness among contending ERDEVs, the maximum number of attempts in a set of ranging round(s) specified by the same RCM is determined by the next higher layer of the controller. This information may be exchanged by the Ranging Contention Maximum Attempts IE (RCMA IE), as described in 7.4.4.41, in the RCM. Furthermore, if the controller knows the identities of the controlees, the RDM IE can be used to allocate ranging roles, that is initiator or responder, among ERDEVs.

6.9.7.2 Ranging block and round structure

A ranging block is a time period for ranging. Each ranging block consists of a whole number of ranging rounds, where a ranging round is a period of sufficient duration to complete one entire range-measurement cycle involving the set of ERDEVs participating in the ranging exchange. Each ranging round is further subdivided into an integer number of ranging slots where a ranging slot is a time period of sufficient duration for the transmission of at least one RFRAME. Figure 6-48j shows the ranging block structure. In this figure, the ranging block is divided into N ranging rounds, each consisting of M ranging slots. The slot duration and the number of slots making up a ranging round can be changed between ranging rounds. This can be achieved by the controller sending an RCM with the modified ranging round configuration whenever a change is required.

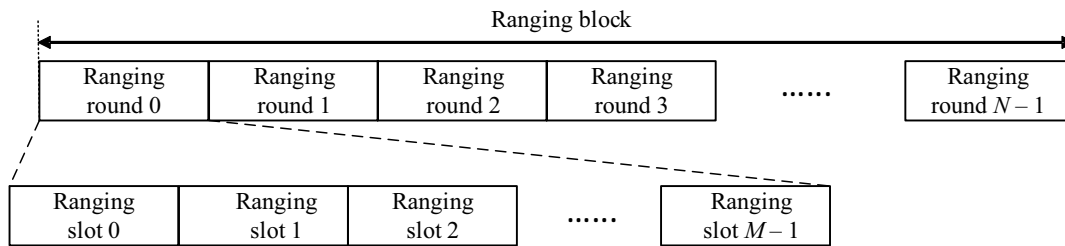


Figure 6-48j—Illustration of ranging block, ranging round, and ranging slot

The time unit used in specifying the duration of ranging block, ranging round, and ranging slot is the RSTU as specified in 6.9.1.5. Ranging devices shall realize this ranging block structure such that the tolerance in the ranging block duration with respect to the PHY clock shall be within ± 100 ppm.

The following nomenclature is used for messages:

- Ranging Control Message (RCM): A message transmitted by a controller in Slot zero, the first slot of a ranging round to configure ranging parameters.
- Ranging Control Update Message (RCUM): A message transmitted by the controller at the last slot of ranging round(s) specified by the RCM to update ranging parameters for the next ranging round(s). The RCUM may include any of the IEs employed by the RCM, to give updates to the values of the parameters conveyed.
- Ranging Interval Update Message (RIUM): A message transmitted by the controller between ranging blocks to update the intervals and also to help the synchronization between the participating ERDEVs. As described in 6.9.7.3.2, the RCUM conveys the scheduled time of the first RIUM, while the RIUM may convey the scheduled time of the next RIUM (if used) before the next ranging block starts.

The following nomenclature is used to describe the functionalities of different exchanges in a ranging round:

- Ranging Control Phase (RCP): A phase in which the controller sends an RCM.
- Ranging Initiation Phase (RIP): A phase in which the initiator(s) sends ranging initiation message(s) to the responder(s).
- Ranging Response Phase (RRP): A phase in which the responder(s) send their response message(s) to the initiator.
- Ranging Final Phase (RFP): A phase in which the initiator sends ranging final message(s) to the responder(s). This phase is only used for DS-TWR.
- Ranging Phase (RP): A phase that should comprise RIP, RRP, and maybe RFP.
- Measurement Report Phase (MRP): A phase in which participating ERDEVs exchange ranging measurements and related service information.
- Ranging Control Update Phase (RCUP): A phase in which the controller sends RCUM. If present, this phase shall be at the last slot of a set of ranging rounds specified by the RCM.
- Ranging Interval Update Phase (RIUP): A phase in which the controller sends RIUM.

In a ranging round SS-TWR or DS-TWR can be used for ranging and localization as described in 6.9.7.4 to 6.9.7.8, or OWR may be used as described in 6.9.1.2.5. As shown in Figure 6-48k, each ranging round may be composed of an RCP, an RP, and an MRP, where each of these phases may consist of multiple slots. In practice, it may be possible to merge some phases. For example, RCP and RIP may be merged into a single

phase when the controller and the initiator are the same device. The MRP may be used to convey ranging-related service information via dedicated IEs.

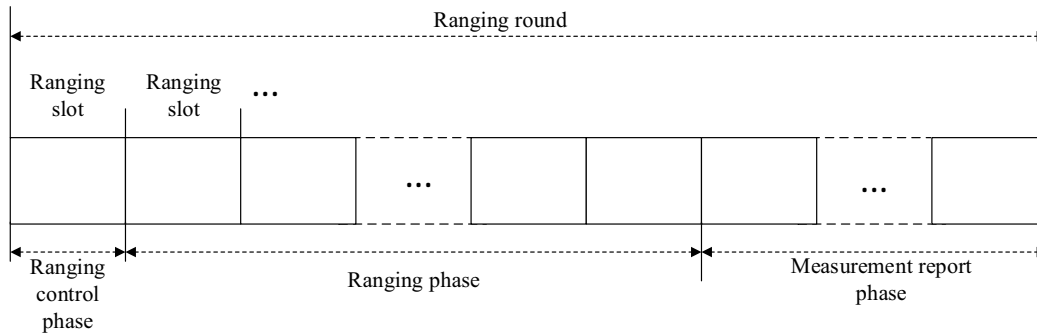


Figure 6-48k—An example of phases in a ranging round

When the Schedule Mode field in the ARC IE is zero, it indicates that contention-based ranging is used. The first ranging slot index and the last ranging slot index for the ranging phase and/or measurement report phase are specified in the RCPS IE (described in 7.4.4.40). The RCPS IE provides the slot indices for the different phases in the ranging round. Where ranging phases for different ranging roles are not specified by the RCPS IE, the ERDEVs may contend for the remaining slots of the ranging round. When the Schedule Mode field in the ARC IE is one, it indicates that time-scheduled ranging is used. In this case, the slot allocation can be specified using the RDM IE (described in 7.4.4.44), or by an out-of-band mechanism.

In Figure 6-48l, message ordering diagrams for different example cases of ranging procedures are presented. In each case, the RCM can be used to indicate the type of ranging that is used.

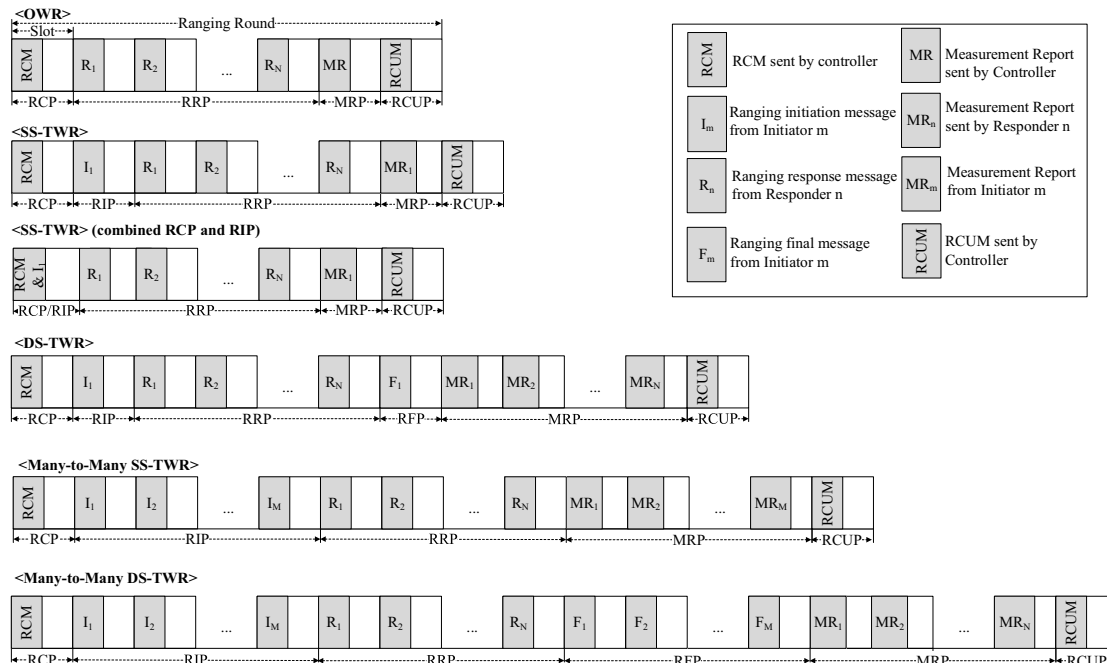


Figure 6-48l—Example timing diagrams for some different multi-device ranging use cases

For ranging with the SP3 format packets, described in 15.2, in addition to the RCP and the RP, the controller may request certain information (e.g., AOA, reply time, or round-trip time measurements) from the controlees participating in the ranging exchange. The controller may send its request in-band as part of the RCM, for example using SP3 Ranging Request Reports IE (SRRR IE) described in 7.4.4.47, or this may be coordinated through some out-of-band mechanism.

Only time-scheduled ranging shall be used for SP3 ranging in order to differentiate messages from different devices. However, the scheduling can be static or dynamic via the RDM IE (described in 7.4.4.44). The scheduling can also be done via an out-of-band mechanism.

SP3 ranging may be performed without a measurement report phase in the ranging round (e.g., an ERDEV can use AOA from multiple ERDEVs to determine location).

One-to-many multi-node ranging with fixed reply times can be supported in the ranging block structure as shown in the example in Figure 6-48m. All packets from the controller and the initiator will follow the slot structure. The i th. responder will respond at fixed reply time FRT_i as shown in Figure 6-48m, where i is from one to N responders. The fixed reply time FRT_j is measured from the RMARKER of the ranging initiation message P1 to the RMARKER of the response message, R_j . Furthermore, the following conditions should be satisfied such that the response frames fit into the allocated slots without overlap:

- $FRT_i > FRT_j$ for $i > j$.
- The time between consecutive ranging transmissions minus the packet length is $\geq K \times RSTU$, where K is a multiplier parameter that depends on the processing capabilities of the ERDEV receiver and chosen by the higher layers at ranging exchange setup.
- $FRT_N + \text{Packet length} < (N + 1) \times \text{Slot length}$.

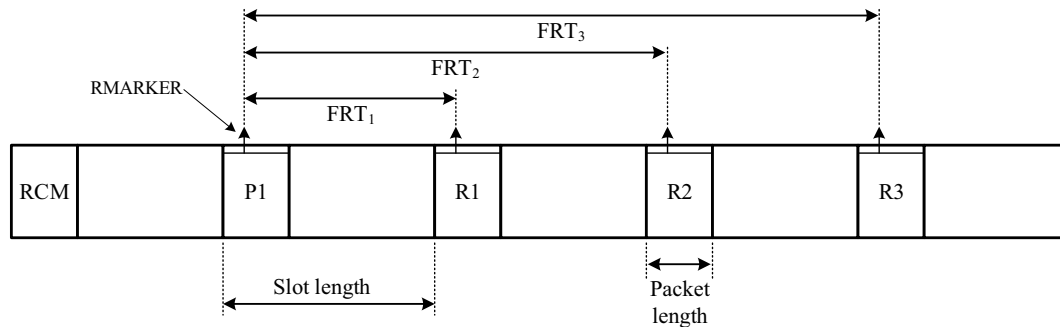


Figure 6-48m—Example ranging round with fixed reply time

The requested fixed reply times can be exchanged via the RRTN IE (described in 7.4.4.49) before the ranging starts or via an out-of-band mechanism.

6.9.7.3 Ranging modes

6.9.7.3.1 Overview

Two different ranging modes are defined: interval-based mode and block-based mode.

The key difference between block-based mode and interval-based mode is that the mean time between successive ranging rounds in block-based mode is assumed to be constant (i.e., using a time structure with uniform spacing), while interval-based mode adopts a time structure with adaptive spacing, and the time between successive ranging rounds may vary dynamically. The next higher layer of the controller selects the

mode and the corresponding time structure. This selection may be achieved by an out-of-band mechanism or in-band using the Time Structure Indicator in the ARC IE as described in 7.4.4.36.

6.9.7.3.2 Interval-based mode

Interval-based mode utilizes the three intervals: block interval, round interval, and RIUM interval. Settings of these intervals are specified in the Ranging Interval Update IE (RIU IE) described in 7.4.4.37.

The following nomenclature is used in this mode:

- Ranging round set: A set of ranging round(s) covered by a specific RCM in a ranging block. Within a ranging round set, ranging rounds are contiguous (i.e., for consecutive ranging rounds, the first ranging slot of the second ranging round immediately follows the last ranging slot of the first ranging round).
- Block interval: Time remaining until the start time of the next ranging block relative to the start time of the current message.
- Round interval: Time remaining until the start time of the ranging round set relative to the start time of the ranging block.
- RIUM interval: Time remaining until the start time of the next RIUM relative to the start time of the current message.

In the first ranging round of a ranging round set, an RCM with the ARC IE (described in 7.4.4.36) configures ranging parameters of the ranging round set. The number of ranging rounds in the ranging round set is specified by the RCM Validity Rounds field of the ARC IE. A ranging block can consist of multiple ranging round sets, while each ranging round set is defined by its RCM at the beginning of the first ranging round of the set.

The controller transmits interval information to controlee(s) using an RIU IE described in 7.4.4.37. The RIU IE can be included in the RCM, RCUM, and RIUM. Upon reception of the RIU IE, each controlee knows the start time of next scheduled ranging round set. The controller can adjust block interval and round interval as a strategy to help reduce interference. The decision criteria and mechanism for adjusting block interval and round interval are out of scope of the standard.

A controlee can request a change to the current ranging configuration by sending a change request with the RCR IE (described in 7.4.4.43), to the controller. The RCR IE can be transmitted along with various IEs to indicate the preferred parameter settings of a controlee, such as the ARC IE (described in 7.4.4.36), the RIU IE (described in 7.4.4.37), the RCPCS IE (described in 7.4.4.48), and the RSKD IE (described in 7.4.4.42). The controller can receive the change request with the preferred ranging parameters in the ARC IE and the preferred intervals in the RIU IE from the controlee. After receiving the change request, the controller should decide whether to accept the change request or not. The controller can transmit an RCUM including IEs with updated ranging parameters. For example, the RCUM can include an RIU IE with updated intervals, which specify the start time of the next ranging block and the ranging round set.

The controller can transmit multiple RIUMs between ranging blocks as shown in Figure 6-48n, each of which contains an RIU IE to indicate the block interval and next round interval values. The Remaining Number of RIUMs field in the RIU IE is decreased in each RIUM sent until it reaches zero, indicating that no more RIUMs should be expected in this ranging block.

Figure 6-48n shows a time diagram example of interval-based mode with one ranging round per ranging block.

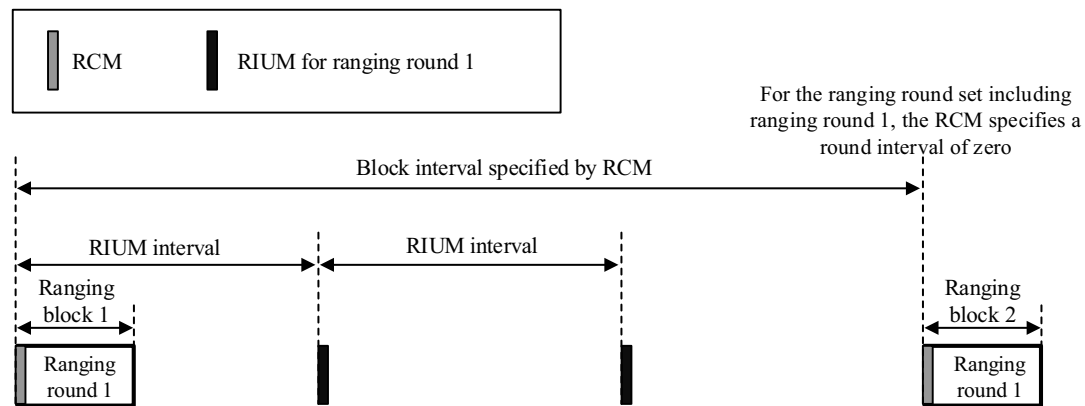


Figure 6-48n—Time diagram for an example of interval-based mode with one ranging round per ranging block

In ranging round one of the first ranging block, the controller transmits an RCM that includes an ARC IE and RIU IE. The ARC IE content (as described in 7.4.4.36) is supplied to the next higher layer of the controlee to set its ranging parameters. Since the RCM covers one ranging round, the RCM Validity Rounds field in the ARC IE is set to one. The various block and round interval values are specified by corresponding fields in the RIU IE. Since the start time of the ranging block and the start time of the RCM are the same, the round interval for ranging round one of the second ranging block is zero. The Next Round Interval field in the RIU IE is zero to specify the round interval for ranging round one of the second ranging block. The controller can transmit RIUMs between ranging blocks. The Block Interval field, the RIUM Interval field, and the Remaining Number of RIUM field are updated in every RIUM.

Figure 6-48o shows a time diagram for an example of interval-based mode with two ranging rounds per ranging block.

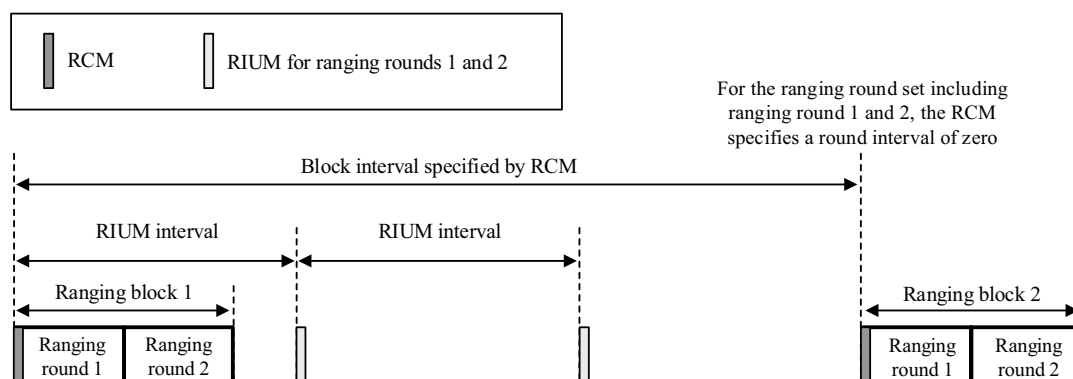


Figure 6-48o—Time diagram for an example of interval-based mode with two ranging rounds per ranging block

In ranging round one of the first ranging block, the controller transmits an RCM that includes an ARC IE (as described in 7.4.4.36) and an RIU IE for ranging rounds one and two. Upon reception of the RCM, the controlees acquire the ranging parameters specified in the ARC IE. Since the RCM covers two ranging rounds, the RCM Validity Rounds field in the ARC IE is two. The various block and round interval values are specified by the corresponding fields in the RIU IE. Since the start times of the subsequent ranging block

and the RCM are the same, the round interval for the ranging round set of the second ranging block is zero. The Next Round Interval field in the RIU IE is zero to specify the round interval for the ranging round set of the second ranging block. The controller can transmit RIUMs between ranging blocks. Block Interval field, RIUM Interval field, and Remaining Number of RIUM field are updated in every RIUM. The second ranging block has two ranging rounds for the same set of ERDEVs in the first ranging block.

Figure 6-48p shows a time diagram for an example of interval-based mode with two ranging round sets per ranging block.

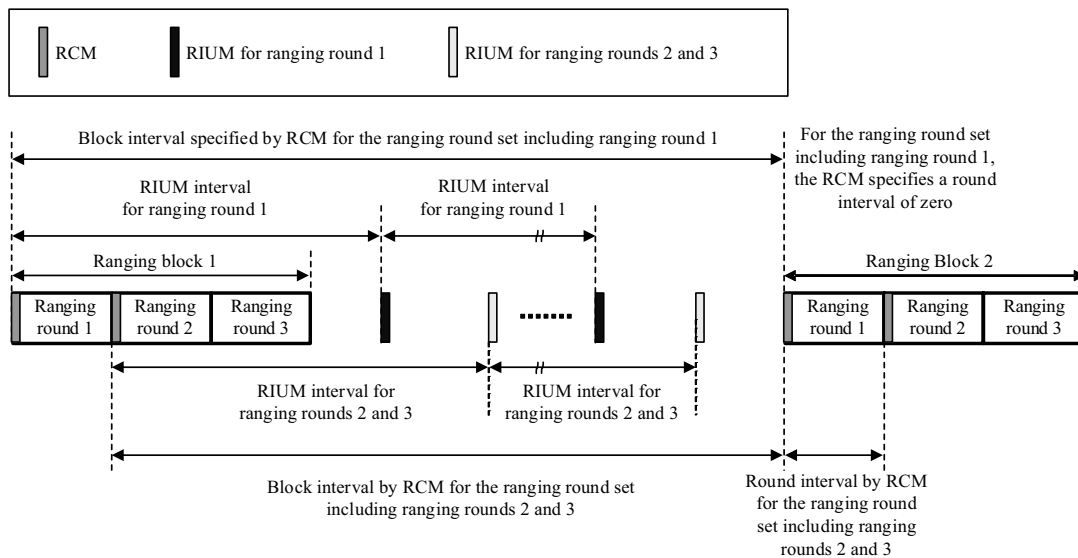


Figure 6-48p—Time diagram for an example of interval-based mode with two ranging round sets per ranging block

The first ranging block has three ranging rounds. In ranging round one in the first ranging block, the controller transmits an RCM that includes the ARC IE (described in 7.4.4.36) and the RIU IE. Upon reception of the RCM, the controlees acquire the ranging parameters specified in the ARC IE. The RCM Validity Rounds field in the ARC IE of the first RCM is one, which indicates that the first RCM covers one ranging round, that is ranging round one. The intervals are specified by the corresponding fields in the RIU IE. Since the start times of the next ranging block and the next RCM for ranging round one are the same, the round interval for ranging round one of the second ranging block is zero. Each RIUM for ranging round one is transmitted with the RIU IE, which specifies the intervals for ranging round one of the second ranging block. Since the second RCM covers two ranging rounds, that is ranging rounds two and three, the RCM Validity Rounds field in the ARC IE of the second RCM is two. Since the start times of the next ranging block and the next RCM for the second ranging round set including ranging rounds two and three are not the same, the round interval for the second ranging round set of the second ranging block is non-zero.

For different ranging round sets in a ranging block, the controller should have the same setting for the Ranging Block Duration field in the ARC IEs conveyed by different RCMs, while other ranging parameters and the participating ERDEVs can be different. For example, the ranging round sets with different ranging parameters can support different sets of ERDEVs with different capabilities, or the same set of ERDEVs for different applications.

If a controlee is not aware of the interval timings, it may recover by continuing to listen to the channel to receive a subsequent RCM.

If a controlee has information for the previous intervals updated by the previous RCM and fails to receive RCM, RCUM, or RIUM with updated intervals, the controlee will continue using the previous intervals.

When the controller updates intervals, it may use the previous intervals to transmit RIUMs including the RIU IE with the updated intervals to the controlee. If the controlee receives the RIUM, it can receive the RCM transmitted by the controller and send its RFRAME in the ranging round with the updated intervals. The controller may stop transmitting the RIUM if the RFRAME from the controlee is successfully received.

RCM Timing Window (RTW) operation is optionally specified by the RIU IE as described in 7.4.4.37. Specifically, a controller can send the RCM at random timing within a time window, namely RTW, centered at its originally scheduled time. The ranging parameters in the ARC IE and the intervals in the RIU IE need to be held constant across the ranging blocks when using RTW operation. The RTW size can be varied for subsequent ranging round sets. The RCM shall be transmitted within the RTW. In order to participate in the exchange, a controlee has to enable its receiver during the RTW in order to receive the RCM.

The controller and the controlee may change the size of the RTW by using the RTW Initial Size field or RTW Multiplier field of the RIU IE. The RTW shall not start before the previous ranging block ends. If the RTW configuration is conveyed by the RIU IE for the subsequent ranging round set, the controller randomly chooses the transmission timing of the next RCM within the RTW. The controlee waits during the RTW to receive the RCM.

Figure 6-48q shows a timing diagram for an example of the RCM transmission with the RTW. RCMs are transmitted at random time within the RTW.

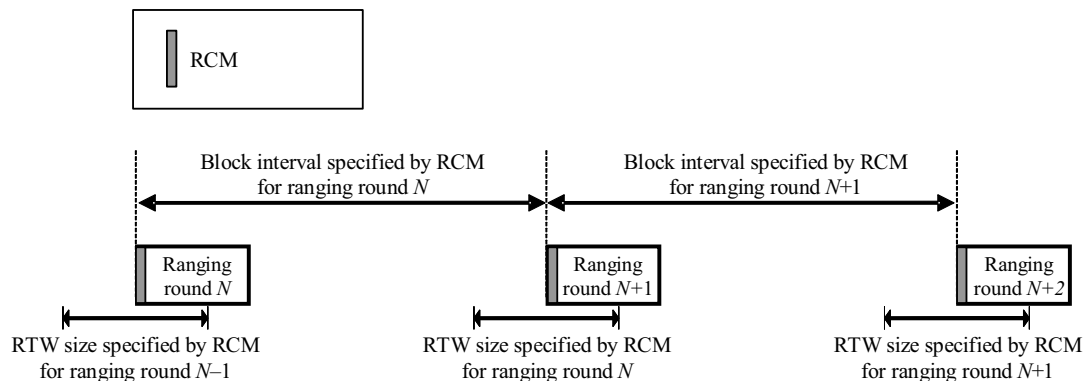


Figure 6-48q—Time diagram for an example of RCM transmission with RTW

Since the ranging parameters in the ARC IE and the intervals in the RIU IE need to be held constant across the ranging blocks during RTW operation, the interval specified by the RCM of ranging round N and the interval specified by the RCM of ranging round $N + 1$ are same. If a controlee fails to receive the RCM of ranging round $N + 1$, the controlee can receive the RCM of ranging round $N + 2$ transmitted at random time within the RTW of ranging round $N + 2$.

6.9.7.3.3 Block-based mode

Block-based mode uses a structured timeline where the ranging block structure, as defined in 6.9.7.2, is periodic by default. Figure 6-48r shows an example timing diagram for block-based mode. The ranging block structure can be setup by specifying the Ranging Block Duration field, the Ranging Round Duration field, and the Ranging Slot Duration field in the ARC IE (as described in 7.4.4.36).

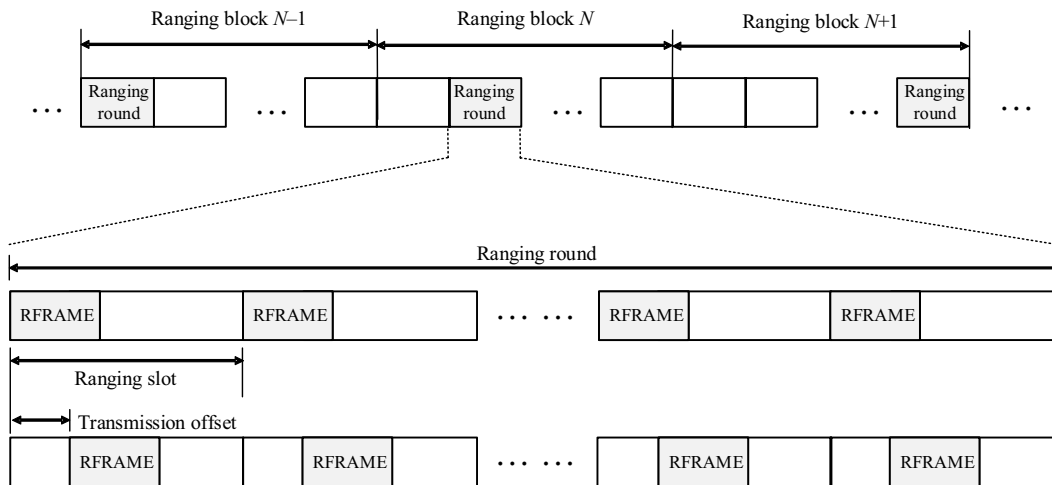


Figure 6-48r—Time diagram for an example of block-based mode

The number of ranging rounds in a ranging block is derived by:

$$\text{Number of ranging rounds} = \frac{\text{Ranging block duration}}{\text{Ranging round duration}}$$

The number of ranging slots in a ranging round is then given by:

$$\text{Number of ranging slots} = \frac{\text{Ranging round duration}}{\text{Ranging slot duration}}$$

These fields completely define the ranging block structure. An ERDEV that receives an RCM successfully may set the initial ranging block structure and the associated timeline for ranging using the values of those ARC IE fields. Alternatively, the ranging block structure may be setup and/or fixed by the next higher layer.

The ranging block structure can be repeatedly transmitted in every RCM by the controller. If the ranging block structure needs to be changed or updated (i.e., to a new ranging block duration, ranging round duration, and/or ranging slot duration), the controller may send a Ranging Block Update IE (RBU IE), as described in 7.4.4.39, to signal the new configuration. In addition to the new block structure configuration, the RBU IE also includes a Relative Ranging Block Index field indicating the number of remaining ranging blocks with the current configuration before switching to the new configuration. The RBU IE can be sent either in the RCM or in the final data frame of a ranging message sequence. Each time the RBU IE is sent, the controller will reduce the Relative Ranging Block Index field by one until it reaches zero. This signals that the next block will be using the new configuration and that the RCM ARC IE in the next block will include the new configuration. Alternatively, the ranging block structure update is signaled to the participating ERDEVs via the next higher layer.

For a given block configuration, each ranging block is referenced by a ranging block index relative to the first block in that configuration (block number zero). Each ranging round in any ranging block is referenced by a ranging round index relative to the first ranging round in the current ranging block. For example, if the ranging block has M ranging rounds, the first ranging round in the block will have ranging round index zero and the last ranging round in the block will have ranging round index $M - 1$. Similarly, each ranging slot in a ranging round is referenced by a ranging slot index relative to the first ranging slot in the ranging round.

For example, in a ranging round with K ranging slots, the first ranging slot in the round will have ranging slot index of zero and the last ranging slot in the round will have ranging slot index $K - 1$. A new ranging message exchange will start by transmitting the first RCM in ranging slot zero of ranging round zero in ranging block zero.

The Ranging Round IE (RR IE), as defined in 7.4.4.38 can be used to signal the ranging round information regarding:

- The current ranging round (i.e., ranging round in the current ranging block i). In this case, the RR IE will be included in the RCM of ranging block i . The transmission of the RR IE in the RCM of the current ranging round will aid the ERDEV to synchronize to the block structure.
- The next ranging round (i.e., ranging round in the next ranging block $i + 1$). In this use case, if the last scheduled message in the current ranging round (of ranging block i) is a message sent by the controller to the controlees, the RR IE will be sent in this final message to signal ranging round information for ranging block $i + 1$. If the last scheduled message in the current ranging round (of ranging block i) is not from the controller but from a controlee, then the controller will send the RR IE in the RCM of the next ranging block (ranging block $i + 1$) to signal the ranging round information for ranging block $i + 2$. In this case, the RCM of ranging block $i + 1$ will have two instances of the RR IE. The first one is applicable to a ranging round in ranging block $i + 1$ and the second one is applicable to ranging block $i + 2$.

In the first ranging round of a ranging message exchange, the RCM packet is transmitted at the beginning of the ranging slot. This RCM will include an RR IE to signal information regarding the ranging round in the current ranging block. In subsequent ranging rounds, the controller may decide to start the transmission within each slot at a different transmission offset. This will be signaled by the controller in the Transmission Offset field of a second instance of the RR IE. This offset should be less than the ranging slot duration minus the UWB packet duration. Figure 6-48s shows an example of ranging rounds with different transmission offsets.

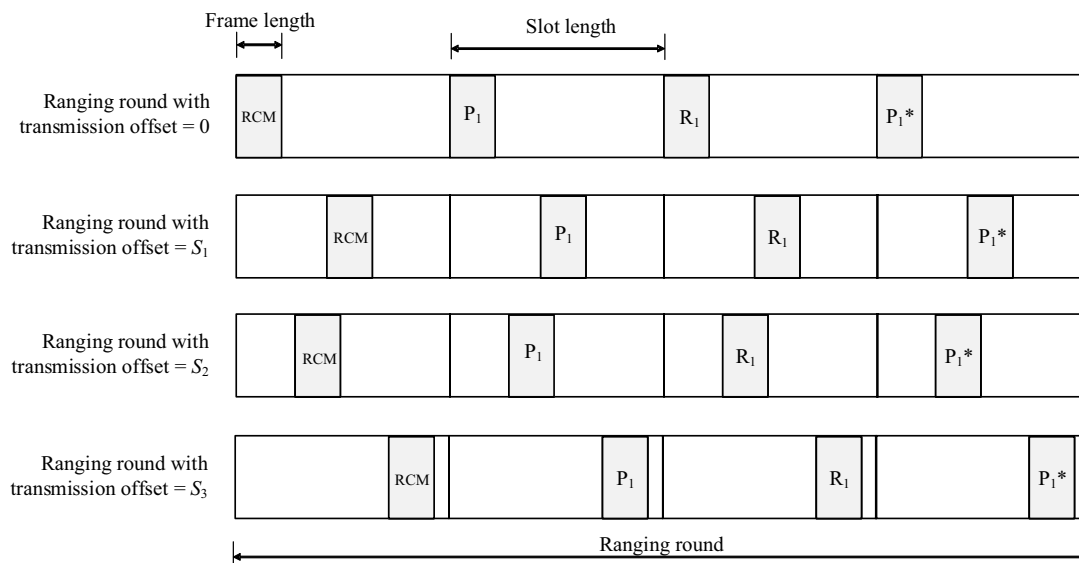


Figure 6-48s—Ranging rounds with different transmission offset

The transmission offset is expressed as a multiple of RSTU. All packet transmissions within the same ranging round should be transmitted with the same transmission offset. The next higher layer of controller is responsible for choosing the transmission offset and communicating it to all other devices in the RR IE. The

controller may change the transmission offset of each ranging round as a strategy to help reduce interference. Controlees should send at the specified offset in their slots, otherwise the packets may be missed by receiving devices expecting the transmission at that offset.

Additionally, participating ERDEVs may continue to use the same ranging round in the next ranging block (i.e., if they are using ranging round m in ranging block n , they will also use ranging round m in ranging block $n + 1$). Alternatively, the controller may decide to “hop” to a different ranging round in the next ranging block (i.e., if participating ERDEVs are using ranging round m in ranging block n , they will use ranging round k in ranging block $n + 1$, where $k \neq m$). Figure 6-48t shows an illustration of the concepts of transmission offset and round hopping. The criteria used to determine when to change the transmission offset and/or hop to a different relative ranging round is outside the scope of the standard and is assumed to be a next higher layer function/protocol. However, it is assumed that as part of such function/protocol, the devices participating in the ranging exchange have either (a) pre-negotiated a hopping sequence that is known to all devices, or (b) have exchanged all the information necessary such that each device can generate the hopping sequence so that they know which ranging round in each ranging block is to be used if hopping is triggered. If the ranging block structure is updated (by sending an RBU IE or by a next higher layer protocol), the participating ERDEVs can set the transmission offset to zero and reset the block, round, and slot indices at the beginning of the new ranging block structure.

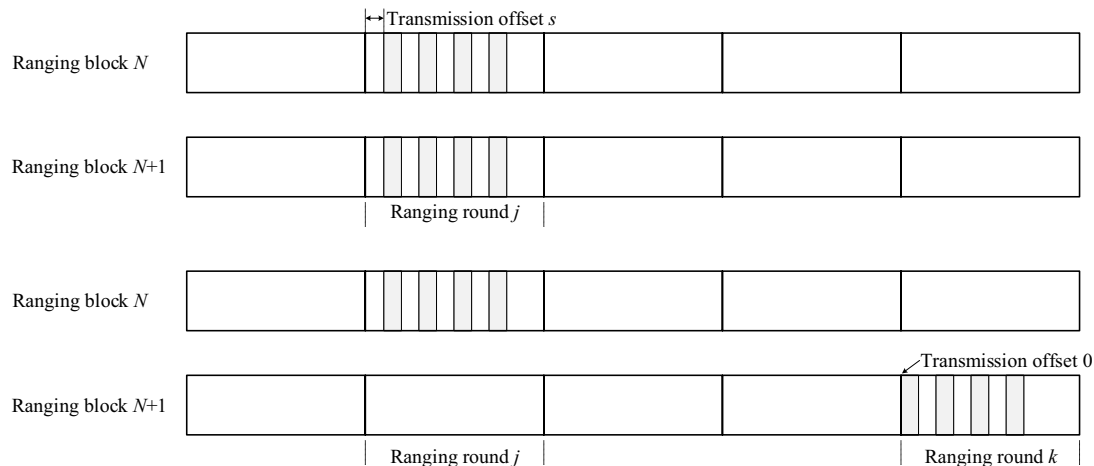


Figure 6-48t—Illustration of transmission offset and round hopping

In the allocated ranging round of a ranging block, the controller configures the ranging round by sending the RCM with the ARC IE (described in 7.4.4.36) and the RR IE (described as defined in 7.4.4.38). The controller next higher layer is responsible for selecting the hopping mode and transmission offset to be used in the ranging round of the next ranging block. If the last scheduled message in the current ranging round in block i is a message sent by the controller to the controlees, then the controller will send the RR IE in this last message of the current ranging round to signal to the participating ERDEVs whether to hop to a different round and/or use a different transmission offset in the ranging round of the next ranging block $i + 1$. If the last scheduled message in the current ranging round is not from the controller, then the controller will send a second RR IE in the RCM of the ranging round in block $i + 1$ to signal to the participating ERDEVs whether to hop to a different round and/or use a different transmission offset in the ranging round of ranging block $i + 2$. Note that in this last case, the RCM in block $i + 1$ will include two instances of the RR IE. The first instance is applicable to ranging in block $i + 1$ while the second instance is applicable to ranging in block $i + 2$. The contents of the RR IE will be the Ranging Block Index field and Ranging Round Index field of the current ranging block, the Hopping Mode field and the Transmission Offset field for the ranging round of the next ranging block. After receiving the RR IE in the final message of a ranging message sequence or as a second RR IE instance in an RCM, the controlee next higher layer is responsible for using the indicated

ranging round and transmission offset in the subsequent ranging block. If the controlee does not receive the RR IE (either in the final message of the exchange or in the RCM), for example due to an interference event, the controlee can turn on hopping in the next ranging block and move to a new ranging round (as determined by the new hopping mode, next ranging block index, and hopping sequence) with a transmission offset of zero. An ERDEV that misses the ARC IE but correctly receives the RR IE in the last message in the current round can use the content of the RR IE to resynchronize to the block structure and be able to receive the RCM and ARC IE in the next ranging block so long as the ranging block structure is unchanged. The ranging block structure, specified by the ARC IE and RR IE sent in the RCM, as well as the RR IE and RBU IE sent either in the last message or in the RCM, allows each participating ERDEV to maintain synchronization with the ranging block structure while being idle with its receiver turned off during unused slots to save energy.

6.9.7.3.4 Receiver enable in slotted ranging schemes

In multi-device slotted ranging schemes rather than leaving the receiver on all the time, the next higher layer can use the MLME-RX-ENABLE.request to enable reception just in the slots where messages are expected to be received. The MCPS-DATA.indication and MLME-RX-ENABLE.indication can be used by the next higher layer to keep track of which slots it receives packets in and which it does not. This is illustrated in Figure 6-48u.

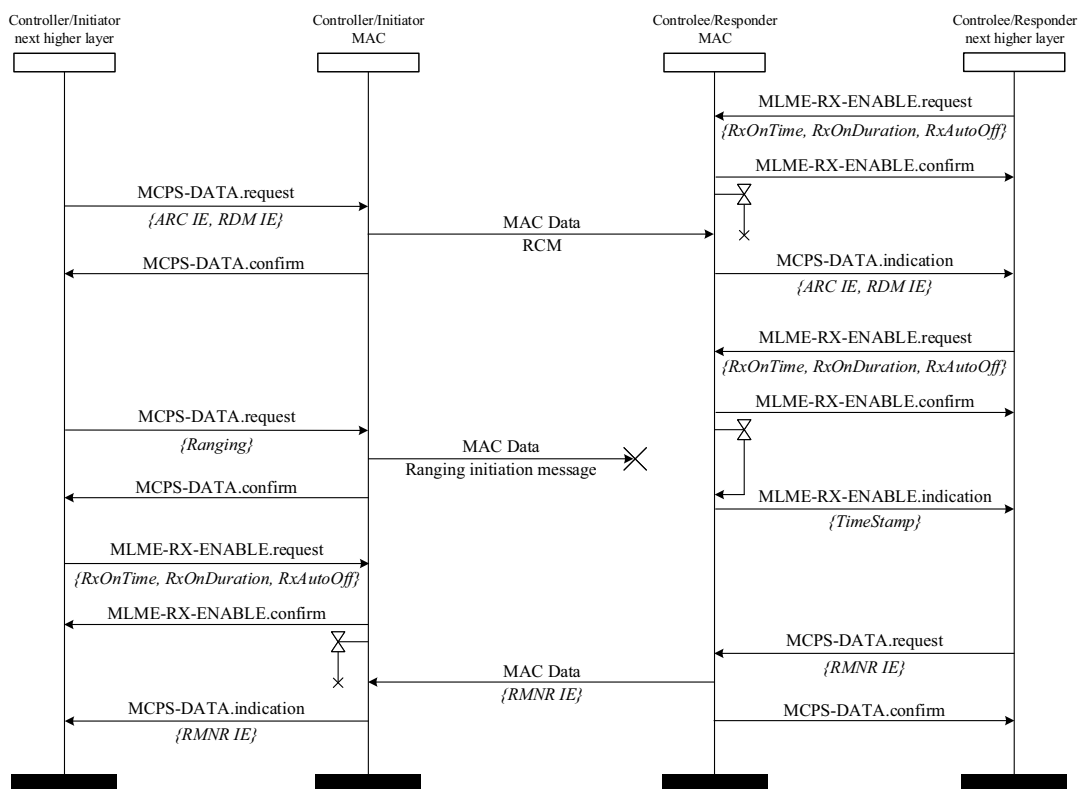


Figure 6-48u—Message sequence chart illustrating MLME-RX-ENABLE.indication use

6.9.7.4 Ranging Procedure for one-to-many SS-TWR

For one-to-many SS-TWR, as shown Figure 6-48v, the example ranging exchange is started by the initiator, where the RRMC IE as described in 7.4.4.45 is embedded in the ranging initiation message broadcast to multiple responders.