**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | IEEE 802.15.4z MAC |
| Date Submitted | June 27th, 2019 |
| Source | Boris Danev (3db Access), Patrick Leu (ETH Zurich), Srdjan Capkun (ETH Zurich), Peter Sauer (Microchip), David Barras (3db Access) |
| Re: | Updated Text for Secure Authenticated Ranging (802.15.4z\_D006e) |
| Abstract | This contribution proposes updated text for the baseline draft 802.15.4z\_D006e |
| Purpose | Provision of the text to facilitate its incorporation into the draft text of the IEEE 802.15.4z standard currently under development in TG4z. |
| Notice | This document does not represent the agreed views of the IEEE 802.15 Working Group. It represents only the views of the participants listed in the “Source(s)” field above. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. |
| Release |  |
| Patent Policy | The contributor is familiar with the IEEE-SA Patent Policy and Procedures:  <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and  <http://standards.ieee.org/guides/opman/sect6.html#6.3>.  Further information is located at <http://standards.ieee.org/board/pat/pat-material.html> and  <http://standards.ieee.org/board/pat>. |



**Add Authenticated Ranging Control IE in 7.4.4 and update Table 7-16:**

**7.4.4.61 Authenticated Ranging Control IE**

The Authenticated Ranging Control IE specifies the supported types of authenticated ranging methods and security levels to be used by the recipient of this IE. The field Security Level is set by the originator to instruct the recipient to generate its response with a secured ranging frame according to Security Level defined in Clause 9.

|  |  |  |
| --- | --- | --- |
| **Bits : 0–1** | **2–4** | **5–7** |
| Authenticated Ranging Method Type | Security Level | Reserved |

**Figure 75—Authenticated Ranging Control IE field format**

**Table (TBD)** **Values of Authenticated Ranging Method**

|  |  |
| --- | --- |
| **Field value** | **Authentication ranging method** |
| 0 | Single-sided ranging (SS-TWR) with one-way authentication |
| 1 | Single-sided ranging (SS-TWR) with mutual authentication |
| 2 | Double-sided ranging (DS-TWR) with one-way authentication |
| 3 | Double-sided ranging (DS-TWR) with mutual authentication |

Remove the following PIBs *secAuthRangingKey, secAuthRangingVUpper96 and secAuthRangingVCounter* from 8.4.2 and revise 8.4.2 MAC PIB attributes list with update text:

**MAC PIB attributes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Attribute** | **Type** | **Description** | **Value** | **Default** |
| *authRangingWithBitErrorsEnabled* | Binary | This attribute enables authenticated ranging with tolerance of bit errors in the cryptographic challenges and responses. | Enabled when TRUE. Otherwise authenticated ranging without errors is used. | FALSE |
| *authRangingSecurityLevel* | Integer | This attribute configures Security Level for authenticated ranging with tolerance of bit errors. It is used in conjunction when *authRangingWithBitErrorsEnabled* is set to TRUE. | This value is 1, 2 or 3 specifying a Security Level of 32, 64 or 128 bits. | 1 |
| *authRangingMode* | Binary | This attribute specifies the authenticated ranging mode when *authRangingWithBitErrorsEnabled* is set to TRUE. | 0: One-way authentication  1: Mutual authentication | 0 |
| *distanceBoundingEnabled* | Binary | This attribute enables distance bounding at the Receiver with a maximum distance decrease based on Tint,RF. Annex G provides normative information on Tint,RF. | Enabled when TRUE. Otherwise distance bounding by distance commitment is disabled. | TRUE |

Replace entire Clause 6.9.9 with the following revised version:

6.9.9 Authenticated Ranging

1. * + 1. Overview

This subclause provides the MAC functional description for challenge-response authenticated ranging based on time-of-flight (ToF) measurement and distance bounding by distance commitment on secured data payload. The authenticated ranging schemes use secured ranging frames which contain verifiable ranging data for validation of the ranging exchange and the corresponding measured distance. The generation and verification of the secured ranging frames relies on the security services provided by Clause 9. Annex G provides normative information about the requirements to achieve distance bounding by distance commitment on the secured data payload.

* + - 1. Secured ranging frames

The supported authenticated ranging schemes make use of ranging frames (RFRAME) and secured ranging frames (SRFRAME). SRFRAME is a ranging frame which data payload is secured by the service of data authenticity and/or data confidentiality depending on the selected Security Level. Its frame structure is depicted in Figure 1.

SRFRAME contains the Auxiliary Security Header, Authenticated Ranging Control IE, Challenge IE and Response IE. It can be either a data frame or Enhanced Ack frame (Enh-Ack). Distance bounding by distance commitment defined in Annex G shall be applied on the Challenge IE and Response IE part of the frame to provide an upper bound of the measured distance.



**Figure 1 – Structure of SRFRAME**

An originator ERDEV starting a ranging exchange is referred to as Verifier. A recipient ERDEV is referred as Prover. The ranging exchange consists of Verifier by sending challenge and Prover responding with a response data. RFRAMEs are typically used for the challenge data, while SRFRAMEs are used for the response data. An SRFRAME can contain Challenge IE, Response IE or both Challenge IE and Response IE depending on the supported scheme in order to embed challenge data, response data or both challenge and response data.

Each supported authenticated ranging scheme defines the content of the RFRAMEs and SRFRAMEs respectively. Frame payload can be optionally included in the frame to transfer additional application specific information.

* + - 1. Security Levels

Authenticated ranging supports Security Levels 1-3 and 5-7. Cryptographic challenges are embedded in the Challenge IE and Response IE. Their length with respect to the Security Level is defined in Table 1. These challenges shall be generated by well-established and industry accepted cryptographically secure pseudo-random number generators (CSPRNG).For example, a CSPRNG is specified in Section 10.2.1 of NIST SP 800-90A Rev. 1. The authenticity of the response and, hence, the distance commitment is provided by the security services in Clause 9.

**Table 1 – Security Levels for authenticated ranging**

|  |  |
| --- | --- |
| **Security Level** | **Cryptographic Challenge** |
| 0 | - |
| 1 | 32-bit Challenge |
| 2 | 64-bit Challenge |
| 3 | 128-bit Challenge |
| 5 | 32-bit Challenge |
| 6 | 64-bit Challenge |
| 7 | 128-bit Challenge |

The lengths of cryptographic challenges with maximum allowed bit errors per Security Level are defined in Table 2. Annex G.3 provides the rationale and mathematical law of the maximum allowed bit errors in the cryptographic challenge.

**Table 2 - Security Levels for authenticated ranging with tolerance of bit errors**

|  |  |  |
| --- | --- | --- |
| **Security Level** | **Cryptographic Challenge** | **Maximum allowed bit errors** |
| 0 |  |  |
| 1/5 | 64-bit Challenge | <= 8 bits |
| 2/6 | 128-bit Challenge | <= 15 bits |
| 3/7 | 256-bit Challenge | <= 31 bits |

* + - 1. Ranging procedures

Authenticated ranging can be realized with SS-TWR and DS-TWR. The SS-TWR modes operate with fixed reply times, as specified in the PHY PIB attribute *phyFixedReplyTime*. The DS-TWR modes do not require a fixed reply time and include the secured exchange of timestamp information.

* + - * 1. SS-TWR with one-way authentication

Figure 2 describes the message exchange for SS-TWR with one-way authentication.



**Figure 2 – Message sequence chart for SS-TWR with one-way authentication**

The Verifier higher layer sets *macMaxFrameRetries* to zero to prevent any retransmission of the challenge and sets *distanceBoundingEnabled*. The Prover higher layer enables ranging with fixed reply time by setting *phyFixedReplyTime* and also*,* enables distance commitment by setting *distanceBoundingEnabled.*

The Verifier sets the type to SS-TWR with one-way authentication and specifies the desired Security Level in the Authenticated Ranging Control IE. It also generates a cryptographic challenge referred to as VChallenge for transmitting in Challenge IE. Upon reception of the last symbol of the RFRAME 1, the Prover starts a timer. The timer stops at the *phyFixedReplyTime* and the Prover acknowledges back by SRFRAME 2 (Enh-Ack) with the Security Level specified in the received Authenticated Ranging Control IE from the Verifier*.*Table 3 summarizes the minimal content of the RFRAME and SRFRAME exchanged during the ranging phase.

**Table 3 Content of Challenge and Response IE for SS-TWR with one-way authentication**

|  |  |  |
| --- | --- | --- |
| **RFRAME #** | **Challenge IE** | **Response IE** |
| 1 | VChallenge | - |
| **SRFRAME** # | **Challenge IE** | **Response IE** |
| 2 | - | VChallenge |

* + - * 1. SS-TWR with one-way authentication and tolerance of bit errors in the challenges

Figure 3 describes the message exchange for SS-TWR with one-way authentication and tolerance of bit errors in the cryptographic challenges exchanged between the Verifier and the Prover.



**Figure 3 – Message sequence chart for SS-TWR with one-way authentication and tolerance of bit errors**

The Verifier higher layer sets *macMaxFrameRetries* to zero to disable retransmission of the challenge. The Verifier and the Prover configure the *authRangingMode* to one-way authentication and enable the mode of tolerance of bit errors by setting *authRangingWithBitErrorsEnabled*. The capability to get all packets from the MAC layer even if there are bit errors is requested by using MLME-RAW-ENABLE.request. The Verifier and the Prover also set *distanceBoundingEnabled* and configure the *authRangingSecurityLevel* to be used during the authenticated ranging exchange. The Prover higher layer enables ranging with fixed reply time by setting *phyFixedReplyTime.*

The Verifier higher layer generates a cryptographic challenge (VChallenge) and sets the Challenge IE in RFRAME 1. Upon reception of the last symbol of the RFRAME 1, the Prover starts a timer. The Prover higher layer generates a cryptographic challenge (PChallenge)and provides it to the MAC layer before the timer expires. The timer stops at the configured *phyFixedReplyTime* and the Prover sends back RFRAME 2 with PChallenge in the Response IE.

To complete the authenticated ranging exchange, the Prover sends to the Verifer SRFRAME 3 with the received VChallenge and its generated PChallenge embedded in the Challenge IE and Response IE secured with the service of data authenticity and security level defined by *authRangingSecurityLevel*.

SRFRAME 3 provides the one-way authentication of the Prover to the Verifier. This frame is preferably sent in-band with higher data coding gain or by out-of-band mechanism, for instance using a different radio. Table 4 defines the content of Challenge IE and Response IE.

**Table 4 – Content of Challenge/Response IE for SS-TWR with one-way authentication and tolerance of bit errors**

|  |  |  |
| --- | --- | --- |
| **RFRAME #** | **Challenge IE** | **Response IE** |
| 1 | VChallenge | - |
| 2 | - | PChallenge |
| **SRFRAME #** |  |  |
| 3 | VChallenge | PChallenge |

* + - * 1. DS-TWR with one-way authentication

Figure 4 describes the message exchange for DS-TWR with one-way authentication and no fixed reply time.



**Figure 4 – Message sequence chart for DS-TWR with one-way authentication**

The Verifier higher layer sets *macMaxFrameRetries* to zero in order to prevent any retransmission of the challenge. The Verifier and Prover also set *distanceBoundingEnabled*.

The Verifier sets the type to S-TWR with one-way authentication and the requested security level in the Authenticated Ranging Control IE and generates a cryptographic challenge for the Challenge IE in RFRAME 1. The Prover sends back SRFRAME2 with the requested Security Level in the received Authenticated Ranging Control IE in RFRAME 1*.* Table 5 summarizes the minimal frame content exchanged during the ranging phase.

**Table 5 – Requirements on Challenge/Response IEs for DS-TWR with one-way authentication**

|  |  |  |
| --- | --- | --- |
| **RFRAME #** | **Challenge IE** | **Response IE** |
| 1 | VChallenge | - |
| **SRFRAME #** | **Challenge IE** | **Response IE** |
| 2 | - | VChallenge |
| 3 | - | - |

SRFRAME 3 sends the timestamp information in a secured frame with data confidentiality using an appropriate IE such as RRTM IE (7.4.4.36) or the RTOF IE (7.4.4.37).

* + - * 1. SS-TWR with mutual authentication

Figure 5 describes the message exchange for SS-TWR with mutual authentication and fixed reply time.



**Figure 5 – Message sequence chart for SS-TWR with mutual authentication**

The Verifier and Prover higher layers set *macMaxFrameRetries* to zero to prevent any retransmission of their corresponding challenges and set *distanceBoundingEnabled*.

The Verifier generates a cryptographic challenge (VChallenge) and set the Authenticated Ranging Control IE for SS-TWR with mutual authentication and requested Security Level and Challenge IE in the RFRAME1. The Prover starts a timer upon reception of the last symbol of RFRAME 1, generates a cryptographic challenge (PChallenge), sets the Challenge IE and Response IE in its SRFRAME 2 secured with Security Level in the received Authenticated Ranging Control IE. When the timer expires, the Prover sends back SRFRAME 2. Upon reception of the last symbol of the SRFRAME 2, the Verifier starts also a timer. The higher layer prepares SRFRAME 3 and provides it to the MAC layer before the timer expires. The timer stops at the configured *phyFixedReplyTime* and the Verifier sends back SRFRAME 3. Table 6 summarizes the minimal content of the RFRAME and SRFRAMEs exchanged during the ranging phases.

**Table 6 – Content of Challenge/Response IEs for SS-TWR with mutual authentication**

|  |  |  |
| --- | --- | --- |
| **RFRAME #** | **Challenge IE** | **Response IE** |
| 1 | VChallenge | - |
| **SRFRAME #** | **Challenge IE** | **Response IE** |
| 2 | PChallenge | VChallenge |
| 3 | VChallenge | PChallenge |

* + - * 1. SS-TWR with mutual authentication and tolerance of bit errors in the challenges

Figure 6 describes the message exchange for SS-TWR with mutual authentication and tolerance of bit errors in the cryptographic challenges exchanged between the Verifier and the Prover.



**Figure 6 – Message sequence chart for SS-TWR with mutual authentication and tolerance of bit errors**

The Verifier and Prover higher layer sets *macMaxFrameRetries* to zero to prevent retransmission of their corresponding challenges. The Verifier and Prover higher layer enables ranging with fixed reply time by setting *phyFixedReplyTime* and also set *distanceBoundingEnabled* and configure the *authRangingSecurityLevel* for the ranging exchange.

The Verifier and the Prover configure *authRangingMode* to mutual authentication and enable the mode of tolerance of bit errors by setting *authRangingWithBitErrorsEnabled*. The capability to get all packets with bit errors from the MAC layer is enabled by using MLME-RAW-ENABLE.request. This is needed to be able to receive RFRAME 1, RFRAME 2 and RFRAME 3 which may contain bit errors and therefore fail FCS check.

The Verifier higher layer generates a cryptographic challenge (VChallenge1) and sets the Challenge IE in RFRAME 1. Upon reception of the last symbol of the RFRAME 1, the Prover starts a timer. The Prover higher layer generates a cryptographic challenge (PChallenge)and provides it to the MAC layer before the timer expires. The timer stops at the configured *phyFixedReplyTime* and the Prover sends back RFRAME 2 with PChallenge in the Response IE. Upon reception of the last symbol of the RFRAME 2, the Verifier starts a timer. The Verifier higher layer generates a cryptographic challenge (VChallenge2)and provides it to the MAC layer before the timer expires. The timer stops at the configured *phyFixedReplyTime* and the Verifier sends RFRAME 3 with VChallenge2 in the Response IE.

To complete the authenticated ranging exchange, the Verifier and the Prover exchange their transmitted and received challenges using SRFRAME 3 and SRFRAME 4 secured with the service of data authenticity defined in the pre-configured *authRangingSecurityLevel*. This exchange provides mutual authentication of the Verifier and Prover. The secured frames are preferably sent in-band with higher data coding gain or by out-of-band mechanism, for instance using a different radio. Table 7 defines the content of Challenge IE and Response IE for each frame.

**Table 7 – Content of Challenge/Response IEs for SS-TWR with mutual authentication**

|  |  |  |
| --- | --- | --- |
| **RFRAME #** | **Challenge IE** | **Response IE** |
| 1 | VChallenge1 | - |
| 2 | - | PChallenge |
| 3 | - | VChallenge2 |
| **SRFRAME #** | **Challenge IE** | **Response IE** |
| 4 | VChallenge1 | PChallenge |
| 5 | VChallenge2 | PChallenge |

* + - * 1. DS-TWR with mutual authentication

Figure 7 describes the message exchange for DS-TWR with mutual authentication. It makes use of two SS-TWR with one-way authentication to provide mutual authentication and distance measurement based on timestamp information exchange.



**Figure 7 – Message sequence chart for DS-TWR with mutual authentication**

The Verifier and Prover enable distance bounding by setting *distanceBoundingEnabled* to TRUE.

The Verifier starts the exchange by setting the Authenticated Ranging Control IE to DS-TWR with mutual authentication and the requested security level and generates a cryptographic challenge to embed in the Challenge IE in RFRAME 1. The Prover sends back SRFRAME 2 secured with Security Level indicated in the received Authenticated Ranging Control IE from RFRAME 1*.*

The same procedure is initiated by the Prover. The Prover starts a ranging exchange by setting the Authenticated Ranging Control IE to DS-TWR with mutual authentication and the requested security level and generates a cryptographic challenge to embed in the Challenge IE in RFRAME 3. The Verifier sends back SRFRAME 4 secured with the requested Security Level in the received Authenticated Ranging Control IE (RFRAME 3)*.* Table 8 summarizes the minimal frame content of the exchanged during DS-TWR with mutual authentication.

**Table 8 – Requirements on Challenge/Response IEs for DS-TWR with mutual authentication**

|  |  |  |
| --- | --- | --- |
| **RFRAME #** | **Challenge IE** | **Response IE** |
| 1 | VChallenge | - |
| **SRFRAME #** | **Challenge IE** | **Response IE** |
| 2 | - | VChallenge |
| **RFRAME #** | **Challenge IE** | **Response IE** |
| 3 | PChallenge | - |
| **SRFRAME #** | **Challenge IE** | **Response IE** |
| 4 | - | PChallenge |
| 5 | - | - |

SRFRAME 5 sends the timestamp information in a secured frame with data confidentiality using an appropriate IE. Examples include RRTM IE (7.4.4.36), RTOF IE (7.4.4.37).