**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 | August 29th, 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>. |



Replace entire Clause 6.9.8 in D2 with the following revised version:

6.9.8.1 Authenticated Challenge-Response Ranging

1. * + 1. Overview

This subclause provides the MAC functional description for authenticated challenge-response ranging (ACRR) based on TOF measurement and distance bounding by distance commitment on data payload between ranging devices acting as Verifier and Prover. The ACRR schemes use the Ranging Verifier MAC command frame defined in 7.5.27 and the Ranging Prover MAC command frame defined in 7.5.28. These contain verifiable ranging data for the validation of the ranging exchange and the corresponding TOF. The generation and verification of these frames is under the control of the MCPS-RANGING-VERIFIER and MCPS-RANGING-PROVER primitives defined in clauses 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.3.10 and 8.3.11, which utilize and rely on the security services provided by clause 9. Annex G provides informative information about authenticated ranging with distance commitment.

The MCPS-RANGING-VERIFIER.request and MCPS-RANGING-PROVER.request primitives each include a SecurityLevel parameter for the next higher layer to select the security level, DistanceCommitmentLevel for the next higher layer to select the level of distance commitment, AuthenticatedChallengeResponseRangingMode for the next higher layer to select the type of ranging method, and a RawMode parameter to control whether the FCS check is enabled or disabled for bit error tolerant ACCR.

MCPS-RANGING-VERIFIER.indication and MCPS-RANGING-PROVER.indication primitives provide the challenge and response data together with the ranging counter information to the next higher layer of Verifier and Prover. The MCPS-RANGING-VERIFIER.confirm and MCPS-RANGING-PROVER.confirm primitives signal the end of the exchange and the disabling of the ranging function, and they provide a status parameter to indicate success or other error condition such as a timeout.

For SS-TWR the configuration of the Verifier and Prover node requires enabling the PHY fixed reply time capability. For DS-TWR the reply time is communicated in a separate secure exchange of information after the ranging exchange and a fixed reply time is not required.

Figure 38 illustrates the basic principle of ranging with a challenge and a response exchange between a Verifier and a Prover with fixed reply time at the Prover.



**Figure 38—Message sequence chart for base ACRR with fixed reply time**

The Prover next higher layer invokes MCPS-RANGING-PROVER.request primitive to prepare the receiver for the ranging exchange.

The Verifier next higher layer initiates the ranging exchange by invoking the MCPS-RANGING-VERIFIER.request primitive. The Verifier MAC sends a Ranging Verifier command with the challenge and the Prover MAC returns a Ranging Prover command with its response after a fixed reply time specified by the corresponding PHY fixed reply time attribute in Table 11-2. For an LRP-ERDEV, the specification of the fixed reply time procedure is described in 19.9 and the values of the fixed reply time are specified by the *phyLrpUwbFixedReplyTime* attribute.

The challenge and response data as well as other configuration parameters depend on the ACRR scheme and are described in 6.9.8.4 for each scheme.

If the Challenge is not received at the Prover device with the Ranging Verifier command both devices will timeout with the confirm primitive and status=TIMEOUT as shown in Figure 38a.



**Figure 38a—Message sequence chart for basic ACRR with Challenge timeout**

If the Ranging Prover command is not received at the Verifier device the Prover device will still indicate a successful data transfer to the Prover next higher layer, but the Verifier device will timeout with the confirm primitive and status=TIMEOUT as shown in Figure 38b.



**Figure 38b—Message sequence chart for basic ACRR with Response timeout**

* + - 1. Security Levels

ACCR supports security levels 1-3 and 5-7, defining the length of the cryptographic challenge and response data as per Table 8. The 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 8—Security levels for ACRR**

| **Security level** | **Length of challenge data, Length of response data (bits)** |
| --- | --- |
| 1 and 5 | 32 |
| 2 and 6 | 64 |
| 3 and 7 | 128 |

The length of cryptographic challenges with maximum allowed bit errors per security level are defined in Table 9. Annex G.3 provides the rationale and mathematical law of the maximum allowed bit errors in the cryptographic challenge.

**Table 9—Security levels for ACRR with tolerance of bit errors**

| **Security level** | **Length of challenge data, Length of response data (bits)** | **Maximum allowed bit errors (bits)** |
| --- | --- | --- |
| 1 and 5 | 64 | 8 |
| 2 and 6 | 128 | 15 |
| 3 and 7 | 256 | 31 |

* + - 1. Coordinating ranging methods and security levels

For successful ACRR interworking the Verifier and Prover devices need to be aligned with respect to the security levels and ranging methods to use. The Authenticated Challenge-Response Ranging Control IE (ACRRC IE) defined in 7.4.4.51 may be used to coordinate these parameter values.

In case that ACRRC IE is used by the Verifier device in the Ranging Verifier command to request a particular ranging mode and/or security level to be executed by the Prover device, then this new configuration shall be used by the Prover MAC instead of any previously set one by the MCPS-RANGING-PROVER.request primitive.

* + - 1. ACRR procedures

Authenticated ranging can be realized with SS-TWR and DS-TWR. The SS-TWR modes operate with fixed reply times. The DS-TWR modes do not require a fixed reply time and include a secure exchange of ranging counter (timestamp) information.

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

Figure 39 describes the message exchange for SS-TWR with one-way authentication.



**Figure 39 – Message sequence chart for SS-TWR with one-way authentication**

The Prover next higher layer invokes MCPS-RANGING-PROVER.request primitive to prepare the receiver for the mode SS-TWR with one-way authentication with desired security level and distance commitment level.

The Verifier next higher layer initiates the ranging exchange by invoking the MCPS-RANGING-VERIFIER.request with the desired security Level and distance commitment level. The Verifier MAC generates a fresh VChallenge and transmits it with the Ranging Verifier command. Optionally ACRRC IE can be used to specify the security level the Prover shall use for its response command message.

The Prover MAC receives the VChallenge and starts the timer of the fixed reply time procedure. After the procedure completes and the timer stops, the Prover MAC layer returns a Ranging Prover command containing the received VChallenge with the specified security level in the MCPS-RANGING-PROVER.request. It also indicates the received VChallenge for the next higher layer use.

If ACRRC IE is used within the Ranging Verifer command and a different security level is specified, then the Prover MAC shall use the security level value in the ACRRC IE signaled by the Verifier. If the security level is 0, the Prover shall not respond and go into Timeout.

Upon reception of the Ranging Prover command, the Verifier MAC indicates the VChallenge and received PChallenge to the next higher layer and confirms the status.

**Table 10—Content of challenge and response for SS-TWR with one-way authentication**

| **Message type** | **Content of the Challenge field  in the Ranging Verifier command** | **Content of the Response field  in the Ranging Prover command** |
| --- | --- | --- |
| Command 1 | VChallenge |  |
| Command 2 |  | VChallenge |

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

Figure 40 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 40 – Message sequence chart for SS-TWR with one-way authentication and tolerance of bit errors**

The Prover next higher layer invokes MCPS-RANGING-PROVER.request primitive to prepare the receiver for the ranging exchange with SS-TWR one-way authentication, desired security level, distance commitment level, and the RawMode parameter set to TRUE to have the FCS check ignored (i.e., tolerance of bit errors in the received challenge and response data).

The Verifier next higher layer initiates the ranging exchange by invoking the MCPS-RANGING-VERIFIER.request with the desired security level, distance commitment level, and the RawMode set to TRUE. The Verifier MAC generates a fresh VChallenge and transmits it with the Ranging Verifier command.

The Prover MAC receives the VChallenge, starts the timer of the fixed reply time procedure and generates a fresh PChallenge. After the procedure completes and the timer stops, the Prover MAC returns a Ranging Prover command containing the PChallenge. The PChallenge and the received VChallenge are indicated to the next higher layer use and the status is confirmed.

To verify the integrity of the measurement at the Verifier, the Prover next higher layer invokes the MCPS-DATA.request primitive to transmit a data frame containing the received VChallenge and PChallenge with security level. Security level of 1 to 3 are sufficient to ensure the integrity of the challenge and the response. This data frame is preferably sent in-band with higher data coding gain mode or by out-of-band mechanism, for instance using a different radio.

**Table 11 – Content of challenge and response for SS-TWR with one-way authentication and tolerance of bit errors**

| **Message type** | **Content of the Challenge field  in the Ranging Verifier command** | **Content of the Response field  in the Ranging Prover command** |
| --- | --- | --- |
| Command 1 | VChallenge |  |
| Command 2 |  | PChallenge |

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

Figure 41 describes the message exchange for DS-TWR with one-way authentication without a fixed reply time. This mode is intended for ranging devices which do not support a fixed reply time with the attribute *phyFixedReplyTimeSupported* equals to FALSE or have longer post-processing time during frame reception.



**Figure 41—Message sequence chart for DS-TWR with one-way authentication**

The Prover next higher layer invokes MCPS-RANGING-PROVER.request primitive to prepare the receiver for DS-TWR with one-way authentication with desired security level and distance commitment level.

The Verifier next higher layer initiates the ranging exchange by invoking the MCPS-RANGING-VERIFIER.request for DS-TWR with one-way authentication with the desired security level and distance commitment level. The Verifier MAC generates a fresh VChallenge and transmits it with the Ranging Verifier command. Optionally ACRRC IE can also be used to instruct the Prover. The TxRangingCounter is confirmed to the next higher layer.

The Prover MAC receives the VChallenge, indicates it to the next higher layer and confirms the RxRangingCounter to the next higher layer. Then it returns a Ranging Prover command containing the received VChallenge with security level. It also confirms the TxRangingCounter to the next higher layer.

Upon reception of the Ranging Prover command, the Verifier MAC indicates the VChallenge and received PChallenge to the next higher layer and confirms the RxRangingCounter.

To complete the ranging scheme, a data frame is initiated by the Prover including the ranging counters with security level. Note that security level of 1 to 3 are sufficient to protect their integrity.

**Table 12 – Content of challenge and response for DS-TWR with one-way authentication**

| **Message type** | **Content of the Challenge field  in the Ranging Verifier command** | **Content of the Response field  in the Ranging Prover command** |
| --- | --- | --- |
| Command 1 | VChallenge |  |
| Command 2 |  | VChallenge |

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

Figure 42 describes the message exchange for SS-TWR with mutual authentication and fixed reply time.



**Figure 42 – Message sequence chart for SS-TWR with mutual authentication**

The Prover next higher layer invokes MCPS-RANGING-PROVER.request primitive to prepare the receiver for SS-TWR with mutual authentication exchange with desired security level and distance commitment level.

The Verifier next higher layer initiates the ranging exchange by invoking the MCPS-RANGING-VERIFIER.request with the desired security Level and distance commitment level. The Verifier MAC generates a fresh VChallenge and transmits it with the Ranging Verifier command. The ACRRC IE can optionally be used to request the ranging mode and security level to be used by the Prover.

The Prover MAC receives the VChallenge, starts the timer of the fixed reply time procedure and generates a fresh PChallenge. After the procedure completes and the timer stops, the Prover MAC returns a Ranging Prover command containing the PChallenge and the received VChallenge with configured security level.

After the reception of the Ranging Prover command, the Verifier MAC starts the timer of the fixed reply time procedure and indicates the received PChallenge and VChallenge to the next higher layer. After the procedure completes and the timer stops, the Verifier MAC returns a Ranging Verififer command containing the received PChallenge and VChallenge with security level and confirms the status to the next higher layer. Security levels of 1 to 3 are recommended to verify the integrity of the exchanged challenges and responses.

After the reception of the Ranging Verifier command, the Prover MAC indicates the received VChallenge and PChallenge, and confirms the status to the next higher layer.

**Table 13 – Content of challenge and response for SS-TWR with mutual authentication**

| **Message type** | **Content of the Challenge field  in the Ranging Verifier command** | **Content of the Response field  in the Ranging Prover command** |
| --- | --- | --- |
| Command 1 | VChallenge |  |
| Command 2 | PChallenge | VChallenge |
| Command 3 | VChallenge | PChallenge |

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

Figure 43 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 43 – Message sequence chart for SS-TWR with mutual authentication and tolerance of bit errors**

The Prover next higher layer invokes MCPS-RANGING-PROVER.request primitive to prepare the receiver for SS-TWR with mutual authentication exchange with desired security level, distance commitment level, and the RawMode parameter set to TRUE to have the FCS check ignored (i.e., tolerance of bit errors in the received challenge and response data).

The Verifier next higher layer initiates the ranging exchange by invoking the MCPS-RANGING-VERIFIER.request with the desired security level and distance commitment level. The Verifier MAC generates a fresh VChallenge1 and transmits it with the Ranging Verifier command.

The Prover MAC receives the VChallenge1, starts the timer of the fixed reply time procedure and generates a fresh PChallenge. After the procedure completes and timer stops, the Prover MAC returns a Ranging Prover command containing the PChallenge.

The Verifier MAC receives the PChallenge, starts the timer of the fixed reply time procedure, indicates the received VChallenge1 to the next higher layer and generates a fresh VChallenge2. After the procedure completes and the timer stops, the Verifier MAC returns a Ranging Verifier command with VChallenge2 and confirms the status to the next higher layer. The Prover MAC receives the Ranging Verifier command, indicates the received VChallenge2 and confirms the status to the next higher layer.

To verify the integrity of the measurement and provide mutual authentication, the Verifier and the Prover exchange their transmitted and received challenges using Data frame 4 (VChallenge1, PChallenge) and Data frame 5 (VChallenge2, PChallenge) with security level. The data frames are preferably sent in-band with higher data coding gain or by out-of-band mechanism, for instance using a different radio. Table 14 defines the content of the commands.

**Table 14 – Content of challenge and response for SS-TWR with mutual authentication and tolerance of bit errors**

| **Message type** | **Content of the Challenge field  in the Ranging Verifier command** | **Content of the Response field  in the Ranging Prover command** |
| --- | --- | --- |
| Command 1 | VChallenge1 |  |
| Command 2 |  | PChallenge |
| Command 3 | VChallenge2 |  |

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

DS-TWR with mutual authentication makes use of two SS-TWR with one-way authentication without a fixed reply time. This mode is intended for ranging devices which do not support a fixed reply time, i.e., the attribute *phyFixedReplyTimeSupported* equals to FALSE or require longer post-processing time during frame reception and therefore need to exchange ranging counter information.

Figure 44 describes the message exchange for DS-TWR with mutual authentication without a fixed reply time.



**Figure 44 – Message sequence chart for DS-TWR with mutual authentication**

The Verifier performs a SS-TWR with one-way authentication with the Prover as described in 6.9.8.1 and both confirm the corresponding ranging counters for the next higher layer. Then the Prover performs a SS-TWR with one-way authentication with the Verifier as well and both confirm the corresponding ranging counters.

The DS-TWR with mutual authentication completes with a data frame initiated by the Prover containing the ranging counters with security level. Note that security level of 1 to 3 are sufficient to verify the integrity of the ranging counter values.

Table 15 summarizes the content of the Ranging Verifier and Ranging Prover commands exchanged during DS-TWR with mutual authentication.

**Table 15 – Content of challenge and response for DS-TWR with mutual authentication**

| **Message type** | **Content of the Challenge field  in the Ranging Verifier command** | **Content of the Response field  in the Ranging Prover command** |
| --- | --- | --- |
| Command 1 | VChallenge1 |  |
| Command 2 |  | VChallenge1 |
| Command 3 | VChallenge2 |  |
| Command 4 |  | VChallenge2 |

* + - * 1. ACRR based SS-TWR with one-way authentication for multiple nodes

Figure 45 shows the message exchange for SS-TWR with one-way authentication with one Verifier and multiple Prover nodes.



**Figure 45—Message sequence chart for ACRR based multi-node SS-TWR with one-way authentication**

The Prover nodes are configured with different *FixedReplyDelayTime (1…N)*, i.e., each Prover is configured with its own fixed reply time such that the response frames do not overlap.

In case of variable PRP as defined in 19.2.5 the response frames may overlap with each other. The *FixedReplyDelayTime* for each Prover device is defined by (*phyFixedReplyTime* =4U)/4\*phyFixedDelayFactor.

In both cases the Verifier MAC captures each *RangingCounter (1…N)* and each *Response (1...N)*. The Prover devices respond to the broadcast address and the Verifier use AddressMask defined with the MCPS-RANGING-VERIFIER.request to accept a range of Prover addresses. The Verifier and Prover Timeout for the ranging frames shall be set accordingly to the N Prover *FixedReplyDelayTime (1…N)* at the Verifier and Prover higher layer.