**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 | March 13th, 2019 |
| Source | Patrick Leu (ETHZ), Srdjan Capkun (ETHZ), Boris Danev (3db Access), Mridula Singh (ETHZ), Marc Roeschlin (ETHZ) |
| 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>. |

Acronyms and abbreviations

DS = Double-sided

OWR = One-way ranging

SRDEV = Secure ranging device

SRFRAME = Secure ranging frame

SS = Single-sided

TWR = Two-way ranging

* + 1. Secure Authenticated Ranging
			1. Overview

This subclause provides the MAC functional description for secure authenticated ranging based on time-of-flight (ToF) measurement. Secure authenticated ranging uses secure ranging frames (SRFRAMEs) which contain verifiable ranging data for execution of the ranging exchange. The generation and verification of SRFRAMEs, as well as the secure consolidation of timestamp information relies on security services defined in Clause 9.

* + - 1. Secure ranging frames

The ranging exchange consists of a verifier V initiating by sending a challenge VChallenge, and a prover P responding with PResponse. If the prover also acts as challenger, PResponse can contain a challenge PChallenge. VChallenge and PChallenge are in the following jointly referred to as Challenge. Secure-ranging (SR) c-data represents the cryptographic data for ranging carried by a given SRFRAME and is composed of a challenge and/or a MIC depending on the secure ranging mode.

A secure ranging frame (SRFRAME) is a ranging frame that contains SR c-data.

* + - * 1. SRFRAME

SRFRAME is a secured ranging frame with a frame payload that starts with SR c-data.



**Figure 1 – SRFRAME MAC Payload**

* + - * 1. NH SRFRAME

SRFRAME is reduced to a SYNC sequence and the SR c-data, referred to as NH (no-header) SRFRAME. The Frame Data consists of SR c-data only.



**Figure 2 – NH SRFRAME**

* + - 1. Security Levels

The Security Levels defined in Clause 9 are specified by the structure of Secure Ranging c-data (SR c-data) to be carried in secure ranging frames.

Security levels 1-3 and 5-7 can support secure ranging if SR c-data is embedded in the private payload. The construction of SR c-data depends on the security level. Depending on whether the SRDEV acts as challenger, responder, or both, SR c-data consists of a Challenge, a MIC, or both.

Secure ranging with one-way and mutual authentication allows the transmission of open payload and/or private payload in addition to the challenge.

**Table 1 – Security levels for secure authenticated ranging with one-way authentication**

|  |  |  |
| --- | --- | --- |
| **Security Level** | **c-data** | **Secure Ranging c-data** |
| 0 | - | - |
| 1 | 32-bit MICk(MHR||Open Payload Field||Private Payload Field) | 32-bit Challenge,MICk(MHR||VChallenge) |
| 2 | 64-bit MICk(MHR||Open Payload Field||Private Payload Field) | 64-bit Challenge,MICk(MHR||VChallenge) |
| 3 | 128-bit MICk(MHR||Open Payload Field||Private Payload Field) | 128-bit Challenge,MICk(MHR||VChallenge) |
| 5 | 32-bit MICk(MHR||Open Payload Field) and ENCk(Private Payload Field) | 32-bit Challenge,MICk(MHR||VChallenge) |
| 6 | 64-bit MICk(MHR||Open Payload Field) and ENCk(Private Payload Field) | 64-bit Challenge,MICk(MHR||VChallenge) |
| 7 | 128-bit MICk(MHR||Open Payload Field) and ENCk(Private Payload Field) | 128-bit Challenge,MICk(MHR||VChallenge) |

**Table 2 – Security levels for secure authenticated ranging with mutual authentication**

|  |  |  |
| --- | --- | --- |
| **Security Level** | **c-data** | **Secure Ranging c-data** |
| 0 | - | - |
| 1 | 32-bit MICk(MHR||Open Payload Field||Private Payload Field) | 32-bit Challenge,MICk(MHR||VChallenge||PChallenge) |
| 2 | 64-bit MICk(MHR||Open Payload Field||Private Payload Field) | 64-bit Challenge,MICk(MHR||VChallenge||PChallenge) |
| 3 | 128-bit MICk(MHR||Open Payload Field||Private Payload Field) | 128-bit Challenge,MICk(MHR||VChallenge||PChallenge) |
| 5 | 32-bit MICk(MHR||Open Payload Field) and ENCk(Private Payload Field) | 32-bit Challenge,MICk(MHR||VChallenge||PChallenge) |
| 6 | 64-bit MICk(MHR||Open Payload Field) and ENCk(Private Payload Field) | 64-bit Challenge,MICk(MHR||VChallenge||PChallenge) |
| 7 | 128-bit MICk(MHR||Open Payload Field) and ENCk(Private Payload Field | 128-bit Challenge,MICk(MHR||VChallenge||PChallenge) |

Challenge length and Security Levels for secure authenticated ranging with tolerance of bit errors are defined in Table 3.

**Table 3 - Security levels for secure authenticated ranging with tolerance of bit errors**

|  |  |  |  |
| --- | --- | --- | --- |
| **Security Level** | **c-data** | **Secure Ranging c-data** | **Error tolerance** |
| 0 | - |  |  |
| 1/5 | - | 64-bit Challenge | <= 8 bits |
| 2/6 | - | 128-bit Challenge | <= 15 bits |
| 3/7 | - | 256-bit Challenge | <= 31 bits |

* + - 1. Generation of Challenges

The challenges are generated using a Deterministic Random Bit Generator (DRBG). The DRBG is based on AES-128 in counter mode. It follows the specification in Section 10.2.1 of NIST SP 800-90A Rev. 1. The counter length is set to 32 bits.

The output of the DRBG is truncated to the desired length of the challenge (32, 64, 128 or 256 bits) depending on the secure ranging mode and Security Level.

**Table 4 - Elements of V and key, both used for challenge generation in secure authenticated ranging**

|  |  |  |
| --- | --- | --- |
| **MAC PIB Attribute** | **Length** | **Description** |
| *secAuthRangingVCounter* | 32 bits | Counter used for DRBG. Initially set to zero. Increased after every DRBG run, i.e., after 128 bits of output. SRDEVs are expected to keep *secAuthRangingVCounter* synchronized. |
| *secAuthRangingVUpper96* | 96 bits | Nonce value that forms V vector together with *secAuthRangingVCounter.* V vector is encrypted with AES-128 under thekey *secAuthRangingKey*.The structure of *secRangingVUpper96* is described below. |
| *secAuthRangingKey* | 128 bits | Symmetric key used to secure authenticated ranging. Either pre-shared or established in-/out-of-band before ranging operation. |



**Figure 3 - Challenge generation for secure authenticated ranging**

* + - * 1. Structure of *secAuthRangingVUpper96*

*secAuthRangingVUpper96* acts as a nonce to prevent forgery of ranging challenges. It is composed of the SRDEV source address and the frame counter.

**Table 5 - Composition of secAuthRangingVUpper96 for secure ranging without bit errors**

|  |  |
| --- | --- |
| **Length: 64 bits** | **32 bits** |
| *Source Address* | *Frame Counter* |

The Source Address field shall be set to the extended address of the device transmitting the frame. The Frame Counter field shall be set to the value of the respective field in the Auxiliary Security Header field, as defined in 9.4.

* + - 1. Ranging Procedures

Secure 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 secure exchange of timestamp information after the secure ranging exchange.

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

Prover (right) authenticates to Verifier (left). This mode is based on a fixed reply at the Prover, as configured in the PIB attribute *phyFixedReplyTime*.

**Table 6 Requirements on SR c-data for secure SS-TWR with one-way authentication**

|  |  |
| --- | --- |
| **NH SRFRAME** | **SR c-data** |
| 1 | VChallenge |
| 2 | VChallenge||MICk(MHR||VChallenge) |



**Figure 4 - MSC for Secure SS-TWR with one-way authentication**

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

The last frame from prover to verifiers carries both VChallenge and PChallenge sent by verifier and prover during the ranging exchange. The dashed box highlights that the last transmission happens on some other error-tolerant UWB link or OOB.

**Table 7 – Requirements on SR c-data for secure SS-TWR with one-way authentication**

|  |  |
| --- | --- |
| **NH SRFRAME** | **SR c-data** |
| 1 | VChallenge |
| 2 | PChallenge |



**Figure 5 - MSC for Secure SS-TWR with one-way authentication and tolerance of bit errors**

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

Prover (right) authenticates to Verifier (left). This mode is not based on a fixed reply time and requires the secure transmission of timestamp information after the ranging exchange. Thereby, timestamp information shall be securely authenticated using the services defined in Clause 9.

**Table 8 – Requirements on SR c-data for secure DS-TWR with one-way authentication**

|  |  |
| --- | --- |
| **SRFRAME** | **SR c-data** |
| 1 | VChallenge |
| 2 | VChallenge||MICk(MHR||VChallenge) |



**Figure 6 - MSC for Secure DS-TWR with one-way authentication**

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

First, the Prover (right) authenticates to the Verifier (left). Then, the verifier (left) authenticates to the prover (right). This mode is based on fixed reply times in both verifier and prover device, as configured in the PIB attribute *phyFixedReplyTime*.

**Table 9 – Requirements on SR c-data for secure SS-TWR with mutual authentication**

|  |  |
| --- | --- |
| **SRFRAME** | **SR c-data** |
| 1 | VChallenge |
| 2 | PChallenge||VChallenge||MICk(MHR||PChallenge||VChallenge) |
| 3 | PChallenge||VChallenge||MICk(MHR||PChallenge||VChallenge) |



**Figure 7 - MSC for Secure SS-TWR with mutual authentication**

* + - * 1. Secure SS-TWR with mutual authentication and tolerance of bit errors

The dashed box highlights that the last two transmission happen on some other error-tolerant UWB link or OOB.

1. **Table 10 – Requirements on SR c-data for secure SS-TWR with mutual authentication**

|  |  |
| --- | --- |
| **NH SRFRAME** | **SR c-data** |
| 1 | VChallenge1 |
| 2 | PChallenge |
| 3 | VChallenge2 |

1. 

**Figure 8 – MSC for Secure SS-TWR with mutual authentication and tolerance of bit errors**

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

This mode is not based on fixed reply times and requires the secure transmission of timestamp information after the ranging exchange. Thereby, timestamp information has to be securely authenticated using the services defined in Clause 9.

**Table 11 – Requirements on SR c-data for secure DS-TWR with mutual authentication**

|  |  |
| --- | --- |
| **SRFRAME** | **SR c-data** |
| 1 | VChallenge |
| 2 | VChallenge||MICk(MHR||VChallenge) |
| 3 | PChallenge |
| 4 | PChallenge||MICk(MHR||PChallenge) |



**Figure 9 - MSC for secure DS-TWR with mutual authentication**

* + - 1. MAC Information Elements
				1. Ranging control

**Table 12** - **Ranging Control IE**

|  |
| --- |
| **Bits: 2** |
| Secure Authenticated Ranging Mode |

Values of the Ranging Mode Field:

* Secure single-sided ranging with one-way authentication, SS-TWR with fixed reply time (default)
* Secure single-sided ranging with mutual authentication, SS-TWR with fixed reply time
* Secure double-sided ranging with one-way authentication, DS-TWR with fixed reply time
* Secure double-sided ranging with mutual authentication, DS-TWR with fixed reply time
	+ - 1. MAC PIB attributes

**Table 13 - MAC PIB attributes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Attribute** | **Type** | **Description** | **Value** |
| *secAuthRangingSecurityLevel* | Integer | Security Level for secure ranging can be configured as PIB attribute in case of OOB configuration. | Depending on the security level, this value is 32, 64 or 128 bits. Default is 128 bits. |
| *secdAuthRangingEnabled* | Binary | Enables maximum distance decrease at the Receiver based Tint\_rf. Annex G provides normative information on Tint\_rf. | Enabled when True. Default is 0, i.e., secure authenticated ranging functionality is disabled. |
| *secAuthRangingWithBitErrorsEnabled* | Binary | For SRDEV, this attribute specifies the challenge length for each security level. | Enabled when True. Default is 0, i.e., secure authentic ranging without errors enabled. |
| *secAuthRangingMode* | Binary | The secure ranging mode can be configured as PIB attribute in case of OOB configuration. This is essential in the case of bit errors. | 0: One-way authentication1: Mutual authentication |
| *secAuthRangingVCounter* | 32-bit unsigned | For SRDEV, this attribute provides read and write access to the 32-bit counter that supplies the lower 32 bits of the 128-bit value V used in the DRBG for generating the Challenge.  | 0 to 232-1 |
| *secAuthRangingVUpper96* | 96-bit unsigned | For SRDEV, this attribute specifies the upper 96-bits of the 128-bit value V used in the DRBG for generating the Challenge.  | 0 to 296-1 |
| *secAuthRangingKey* | 128-bit unsigned | For HRP-SRDEV, this attribute specifies the key used in the DRBG for generating the Challenge.  | 0 to 2128-1 |