**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | Change Proposal for Secure Authenticating Ranging using LRP UWB PHY |
| Date Submitted | [06 July, 2018] |
| Source | Prof. Dr. Srdjan Capkun (ETH Zurich)Prof. Dr. David Basin (ETH Zurich)Dr. Boris Danev (3db Access)Prof. Dr. Markus Kuhn (University of Cambridge)Shuiping Long (Huawei Technologies)Yunsong Yang (Futurewei Technologies)Bernd Baer (Marquardt)Matthias Reinhardt (Daimler)Andy Ward (Ubisense)Peter Sauer (Microchip Technology)Paul Studerus (Dormakaba)Mihai Barbulescu (Dormakaba) |  |
| Re: | [If this is a proposed revision, cite the original document.][If this is a response to a Call for Contributions, cite the name and date of the Call for Contributions to which this document responds, as well as the relevant item number in the Call for Contributions.][Note: Contributions that are not responsive to this section of the template, and contributions which do not address the topic under which they are submitted, may be refused or consigned to the “General Contributions” area.] |
| Abstract | [Proposal for Secure Authenticated Ranging based on LRP UWB PHY 802.15.4z] |
| Purpose | [Propose elements of Secure Authenticated Ranging PHY/MAC descriptions] |
| Notice | This document has been prepared to assist the IEEE P802.15. 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 | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. |

6.17 Secure authenticated ranging

Secure authenticated ranging is a round-trip-time ranging using a challenge-response one-way authentication and/or mutual authentication mechanism.

Secure authenticated ranging uses the MAC sublayer providing the security services defined in Clause 9. Secure ranging is provably secure only in LRP UWB Base Mode and Dual-Frequency Mode as defined in Clause 19. Secure authenticated ranging provides the highest security guarantees as defined by the Security Levels of the MAC sublayer in Table 9-6. The Security Levels are ordered as defined in 9.4.1.2.

Secure authenticated ranging uses data frames as defined in 7.3.2 and shall be formatted as illustrated in Figure 7-14. Given that data frames for secure authenticated ranging are not specified in Table 9-1, the Private Payload shall be set to the MAC Payload field and Open Payload field shall be empty as defined in 9.2.1 f).

Secure authenticated ranging devices shall have *macSecurityEnabled* attribute set to TRUE and provide cryptographic transformations on incoming and outgoing frames using information in the PIB attributes associated with security services defined in Clause 9. Alternatively, if *macSecurityEnabled* attribute is set to TRUE, secure authenticated ranging is enabled.

**[Comment<1>:** DefineIEto indicate one-way vs. mutual authentication**]**

**6.17.1 Secure ranging with one-way authentication**

This subclause describes the two-way message exchange based on AES CCM\* security services in 9.1 in order to achieve secure ranging with one-way authentication.



Figure 1- Secure ranging with one-way authentication

**6.17.1.1 VNonce**

VNonce is a fresh random number of 32, 64 or 128 bits corresponding to the chosen Security Level. The generation mechanism is outside the scope of this standard.

|  |  |
| --- | --- |
| **VNonce** | **Length (bits)** |
| VNonce32 | 32 |
| VNonce64 | 64 |
| VNonce128 | 128 |

The Security Level shall be set to 0 in the Security Control field of the Auxiliary Security Header. This indicates that VNonce is neither authenticated, nor encrypted data, i.e., no CCM\* transformation is performed on the VNonce.

**6.17.1.2 PResponse**

PResponse is the *c* data containing the MIC (Message Integrity Code) as defined in Table 9-4. Table X defines the *a*data to be used for the CCM\* transformation to compute the *c* data. VNonce is the Unsecured Private Payload field defined in Table 9.3.

|  |  |  |  |
| --- | --- | --- | --- |
| Security level | *a* data | *m* data | *c* data (PResponse) |
| 0 | Not applicable | Not applicable | Not applicable |
| 1 | MHR || VNonce32 | None | MIC-32 |
| 2 | MHR || VNonce64 | None | MIC-64 |
| 3 | MHR || VNonce128 | None | MIC-128 |

NOTE—The MHR contains the Auxiliary Security Header field, as defined in 7.2

**6.17.2 Secure ranging with mutual authentication**

This subclause describes the three-way message exchange based on AES CCM\* security services in 9.1 in order to achieve secure ranging with mutual authentication.



Figure 2 Secure ranging with mutual authentication

**6.17.2.1 VNonce**

VNonce is a fresh random number of 32, 64 or 128 bits corresponding to the chosen Security Level. The generation mechanism is outside the scope of this standard.

**6.17.2.2 PNonce**

PNonce is a fresh random number of 32, 64 or 128 bits corresponding to the chosen Security Level. The generation mechanism is outside the scope of this standard.

**6.17.2.3 PResponse**

PResponse is the *c* data containing the MIC (Message Integrity Code) as defined in Table 9-4. Table X defines the *a*data to be used for the CCM\* transformation to compute the *c* data. VNonce is the Unsecured Private Payload field defined in Table 9.3.

|  |  |  |  |
| --- | --- | --- | --- |
| Security level | *a* data | *m* data | *c* data (PResponse) |
| 0 | Not applicable | Not applicable | Not applicable |
| 1 | MHR || PNonce32 || VNonce32 | None | MIC-32 |
| 2 | MHR || PNonce64 || VNonce64 | None | MIC-64 |
| 3 | MHR || PNonce128 || VNonce128 | None | MIC-128 |

NOTE—The MHR contains the Auxiliary Security Header field, as defined in 7.2

**6.17.2.4 VResponse**

VResponse is the *c* data containing the MIC (Message Integrity Code) as defined in Table 9-4. Table X defines the *a*data to be used for the CCM\* transformation to compute the *c* data. VNonce is the Unsecured Private Payload field defined in Table 9.3.

|  |  |  |  |
| --- | --- | --- | --- |
| Security level | *a* data | *m* data | *c* data (PResponse) |
| 0 | Not applicable | Not applicable | Not applicable |
| 1 | MHR || VNonce32 || PNonce32  | None | MIC-32 |
| 2 | MHR || VNonce64 || PNonce64 | None | MIC-64 |
| 3 | MHR || VNonce128 || PNonce128  | None | MIC-128 |

NOTE—The MHR contains the Auxiliary Security Header field, as defined in 7.2

**6.17.3 Distance commitment**

Distance commitment ensures that the data of the PSDU carrying the nonces and MIC of the MAC payload is decoded at the measured distance by the first path. This is essential to secure authenticated ranging and provable security as defined in Annex G.

Figure 3 illustrate the distance commitment. Channel state information (channel impulse response) shall be available after the SHR. The first path is detected from the channel state information. During reception of PSDU only the “first path” portion of the received signal shall be used for data decoding.

**[Comment<2>:** Consider more precise definition of “first path” portion in order to ensure strict security guarantees between different chip vendors**]**



Figure 3 Distance commitment

**6.17.4 Protocol verification**

Verification for success or failure is performed by the Verifier in the one-way authentication and by both the Verifier and the Prover in the mutual authentication.

The verification procedure of secure authenticated ranging consists of bit-wise matching the received nonces and computed MIC.

**[Comment<3>:** Include a section on the type of shared keys to be used. Especially, mandate the use of only link keys (i.e., pair-wise shared keys) between devices and not group keys. Keys shared by a group of devices can be subject to insider attacks, i.e., the attacker can impersonate as an innocent device, associate with the group, thereby obtain the group key for launching the forgery attacks.**]**

Annex G (normative) Security guarantees of secure authenticated ranging

**Protocols/Logical Layer:**

The presented secure ranging protocols are natural extensions of one-way and mutual authentication protocols. However, since the analysis of ranging protocols includes notions of time and distance, proving their security requires being able to reason about such notions. [TISSEC2011] presents a formal model for the analysis of such protocols. In particular, it describes (Section 3) and formally proves the security of a signature-based “authenticated ranging protocol” (Section 5.1). Secure ranging with one-way authentication described in this standard (6.17.1) aims to achieve the same security properties as authenticated ranging, namely, authentication and prevention of any distance reduction attacks. Namely, assuming mutually trusted parties, their measured distance should constitute an upper bound on their actual distance. The only difference between the two protocols is that for message authentication, the protocol in the standard uses a Message Integrity Code (based on the shared secret keys), and includes principal names in the messages, as opposed to the protocol in [TISSEC2011] which relies on public-key signatures. Given this, the formal proof can be easily extended to cover the protocol described in the standard and the results naturally carry over.

The proofs in [TISSEC2011] are done in the symbolic model, assuming that the cryptographic primitives (i.e., signature and MIC) are ideal. This means that the nonces, signatures and MICs are assumed to be unguessable and unforgeable. The protocols are therefore proven secure under that assumption. Assuming that the signature and MIC cannot be forged by the attacker (without the knowledge of the key), the remaining ways for the attacker to violate the security guarantees of these protocols are by guessing the nonces/MICs or by collecting all nonce/MIC pairs. The guessing probabilities of such an attack, for different nonce and MIC sizes are given in Table 1. If the nonce is large enough or if the system rate limits the interactions, then the attacker cannot collect all or most nonce and MIC pairs. The security reasoning for the secure ranging with mutual authentication follows the same reasoning. Namely, this protocol simply combines two one-way secure ranging protocols.

Assuming that the devices can support public key signatures, the proposed protocols can be simply used with public key signatures, replacing MICs. This design is proven in [TISSEC2011].

**Physical Layer:**

In [ESAS2006] the authors argued that, if implemented naively, secure ranging protocols will be vulnerable to physical layer attacks. Most prominent of these attacks is the early detect / late commit attack that exploits long symbols and allows the attacker to cheat on the distance up to the symbol length even if the logical layer protocol is secure.
One safe way to prevent such attacks is to use short symbols (only few ns long). In that case, the attacker can cheat up to few nanoseconds. For an LRP UWB system this means that the attacker’s ability to cheat will depend on the pulse duration and therefore be proportional to the bandwidth of LRP UWB (400MHz – 2.14GHz). The corresponding range of the maximum distance decrease for different bandwidth is given in Table 1. For a bandwidth of 2.14 GHz the maximum distance decrease is 14 cm whereas for 400MHz it is 75cm. These are worst-case numbers. In all realistic scenarios, where the attacker has non-zero detection and non-zero processing time, the maximum distance decrease will be lower.

The secure ranging design in described in 6.17.3 follows the *distance commitment* design that was first described in [WISEC15]. A distance commitment allows a sender to claim to be in a certain distance (by the transmission time of the preamble), which he has to prove later by supplying the correct secret at the correct time on the channel.
The exact transmission timing of the preamble tells the receiver when to sample the channel to extract symbols to demodulate. In this sense, it is a commitment by the sender to send the data at exactly those times, as defined by the physical-layer protocol. The receiver will start sampling the channel for each symbol with timing as defined by the arrival of the preamble. In other words, the insecure distance measurement based only on the preamble simplifies and enables the secure distance measurement by providing correct synchronization. If the preamble is sent earlier by the attacker, the receiver will expect the data pulses earlier as well and thus start the sampling intervals earlier. If the attacker cannot provide correct data pulses in these earlier sampling intervals (e.g., because the prover did not send them yet), the receiver will demodulate random data. Even if he advances the preamble, the attacker therefore cannot cheat on the distance since it cannot provide the correct data (nonce and MIC) before they are sent by V or P.

Table 1.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Level | Nonce length (bits) | Probability of guessing the nonce | Forging of MIC(as per AES CCM\* in Clause 9) | Worst Case Maximum Distance Decrease (1) |
| 0 | Not applicable | Not applicable | Not applicable | Not applicable |
| 1 | 32 | 1/2^32 (2.32e-10) | MIC-32 | 14 cm – 75 cm |
| 2 | 64 | 1/2^64 (5.42e-20) | MIC-64 | 14 cm – 75 cm |
| 3 | 128 | 1/2^128 (2.93e-39)  | MIC-128 | 14 cm – 75 cm |

*Footnote 1: Worst Case Maximum Distance Decrease for strongest theoretical attacker with zero detection time and zero processing time is proportional to the bandwidth of LRP UWB ranging from 400 MHz to 2.14 GHz*

[TISSEC2011] David A. Basin, Srdjan Capkun, Patrick Schaller, Benedikt Schmidt, Formal Reasoning about Physical Properties of Security Protocols. ACM Trans. Inf. Syst. Secur. 14(2): 16:1-16:28 (2011)

[WISEC15] Nils Ole Tippenhauer, Heinrich Luecken, Marc Kuhn and Srdjan Capkun, UWB Rapid-Bit-Exchange System for Distance Bounding, In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2015

[ESAS2006] Jolyon Clulow, Gerhard P. Hancke, Markus G.Kuhn, and Tyler Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS), 2006.