**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |
| --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) |
| Title | **Authenticated Ranging of IEEE 802.15.4** |
| Date Submitted | 17 January, 2019 |
| Source | Prof. Dr. Srdjan Capkun (ETH Zurich)Prof. Dr. David Basin (ETH Zurich)Dr. Boris Danev (3db Access)Institute of Information SecurityCNB F 102.2Universitaetstrasse 68092 ZürichSwitzerland | Voice: +41 44 632 71 90Fax: E-mail: srdjan.capkun@ethz.ch |
| Re: | Authenticated challenge-response ranging |
| Abstract | Authenticated ranging protocols are a set of protocols from the family of distance bounding protocols that provide authentication and protection against distance manipulation attacks on ranging performed between a pair of mutually trusted devices. When distance commitment is used on the PHY layer, these protocols provide both authentication and protection against distance decreasing attacks. References to the related scientific publication where the schemes are described in detail including formal security proofs are provided. |
| Purpose | Best practices for implementing authenticated ranging and security analysis of authenticated ranging schemes |
| 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. |

Authenticated ranging protocols and distance commitment

**1. Authenticated ranging protocols**

Authenticated ranging protocols are a set of protocols from the family of distance bounding protocols that provide authentication and protection against distance manipulation attacks on ranging performed between a pair of mutually trusted devices (*Range Authentication Protocols for Localization* [B1], *Formal Reasoning about Physical Properties of Security Protocols* [B2]). Authenticated ranging schemes in 6.9.9 are natural extensions of one-way and mutual authentication challenge-response protocols. These schemes achieve robustness against distance reduction attacks by using the security services provided in Clause 9: challenge/response for data integrity on the MAC layer and distance commitment on the PSDU (data payload) for range verification.

A formal model for the analysis of authenticated ranging including the notions of time and distance is presented in (*Formal Reasoning about Physical Properties of Security Protocols* [B2]). Ranging with one-way authentication described in 6.9.9.4.1 supports one-way authentication and an upper bound on the distance assuming mutually trusted parties. The arguments are provided in Section 3 and 5.1. The only difference between the scheme in (*Formal Reasoning about Physical Properties of Security Protocols* [B2]) and the scheme in 6.9.9.4.1 is that for message authentication, 6.9.9.4.1 uses a shared key-based Message Integrity Code based AES-CCM\* described in Annex B and includes principal names in the messages, as opposed to relying on public-key signatures. Given this, the theoretical considerations and the results naturally carry over. Ranging with mutual authentication follows the same reasoning by combining two one-way authenticated ranging exchanges.

The cryptographic challenges as well as the secured frames embedding a MIC are assumed to be unguessable and unforgeable. Assuming that the MIC cannot be forged by the attacker (without the knowledge of the key), the remaining ways for the attacker to violate the properties of these protocols are by guessing the challenges and MICs or by collecting all challenge/MIC pairs. If the challenge is large enough or if the system rate limits the interactions, then nonce and MIC pairs will not repeat, thus preventing replay attacks.

**2. Distance commitment**

A threat model, attacks and principles to protect the distance measurement against manipulation are presented in (*So near and yet so far: Distance-bounding attacks in wireless networks* [B3]). Most prominent attacks include deferred bit signaling and early bit detection that exploit the fact that the RF energy in a data symbol is spread over symbol length. This allows an attacker to shorten the time of arrival estimation (and thus reduce the distance) up to the RF symbol duration.

Distance commitment (Section 8.2 in *UWB Rapid-Bit-Exchange System for Distance Bounding* [B4] ) on the payload is one of the measures that enhances authenticated ranging in order to prevent attacks described in (*So near and yet so far: Distance-bounding attacks in wireless networks* [B3]). Distance commitment allows an originator to claim to be in a certain distance (defined by the transmission time of the preamble), which the originator has to verify later by supplying the correct secret at the correct time in the secured data payload. The exact transmission timing of the preamble tells the receiver when to sample the channel to extract symbols to decode. In this sense, it is a commitment by the originator to send the data at exactly those times. The recipient will start sampling the energy for each symbol with timing as defined by the arrival of the preamble. 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 in these earlier sampling intervals (e.g., because the originator did not send them yet), the recipient will decode random data. Even if the attacker advances the preamble, he would need to be able to guess the symbols carrying the cryptographic challenge and response data and corresponding MICs (Clause 9).

The worst case maximum distance manipulation depends on the aperture Tint,RF of the window collecting and integrating the incoming RF energy at the receiver. The window of duration Tint,RF is placed at the expected position in time of the incoming data. An LRP-ERDEV can implement a window duration Tint,RF that corresponds to a maximum distance decrease an application can tolerate.

The theoretical maximum distance decrease is defined by:

Δdmax = c0∙Tint,RF,

where c0 is the speed of light and processing delay equal to zero (*So near and yet so far: Distance-bounding attacks in wireless networks* [B3]).

Longer durations can be used to trade-off distance manipulation resilience (i.e., maximal distance reduction) against energy integration (e.g., which increases sensitivity coming from multipath). UWB LRP PHY with its intrinsic short active time enables minimal Tint,RF.. Other PHYs exist with sufficiently short active RF duration and may support distance commitment.

Table 1 provides the worst case maximum distance decrease when distance commitment is used on the cryptographic challenge and response payload with given number of bits.

**Table 1** – Worst case maximum distance decrease when Tint,RF is equal to the inverse of the bandwidth of UWB pulse ranging from 400 MHz to 2.14 GHz.

|  |  |  |  |
| --- | --- | --- | --- |
| Challenge (bits) | Probability of guessing the challenge | Forging of MIC(as per AES CCM\* in Clause 9) | Worst Case Maximum Distance Decrease |
| 32 | 1/2^32 (2.32e-10) | MIC-32 | 14 cm – 75 cm |
| 64 | 1/2^64 (5.42e-20) | MIC-64 |
| 128 | 1/2^128 (2.93e-39)  | MIC-128 |

**3. Cryptographic challenge length**

Authenticated ranging carries cryptographic challenges with a certain length corresponding to a desired protection against guessing. Cryptographic challenges (also referred to as nonces) can support bit errors and achieve the desired probability of guessing provided that the number of bits of the challenge (Nnonce) is correctly dimensioned with respect to the number of allowed bit errors (Nerr). The choice of Nnonce and Nerr follows the binomial distribution (Section 3.1 of *Secure Neighbor Discovery and Ranging in Wireless Networks* [B5]).

Annex A

[B1] Catherine Meadows, Paul Syverson, Range Authentication Protocols for Localization, 2007

[B2] 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)

[B3] 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.

[B4] 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

[B5] Marcin Poturalski, Secure Neighbor Discovery and Ranging in Wireless Networks, Ph.D. dissertation, EPFL\_TH5131 (2011), https://infoscience.epfl.ch/record/166938/files/EPFL\_TH5131.pdf