Annex G

(normative)

Authenticated Ranging with Distance Commitment

**G.1 General**

Authenticated ranging protocols are a set of protocols from the family of distance bounding protocols that provide authentication and prevent distance manipulation attacks on ranging performed between a pair of mutually trusted devices [B24], [B25]. 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 data payload for range verification (described in this annex).

[B25] presents a formal model for the analysis of authenticated ranging including the notions of time and distance. 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 sections 3 and 5.1. The only difference between the scheme in [B25] 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 the scheme in [B25] which relies 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.

It shall be noted that the cryptographic challenges in Challenge IE and Response IE 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.

[B26] defines threat model, attacks and principles to protect the distance measurement against manipulation. 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 [B27] on the payload is one of the measures that enhances authenticated ranging in order to prevent attacks described in [B26]. 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 cryptographic challenges in Challenge IE and Response IE and the corresponding MICs (Clause 9).

**G.2 Distance Commitment on Data Payload**

The ranging frame data contained in the Challenge IE and Response IE is decoded by capturing only the energy corresponding to the short active RF period of each data symbol sent at a particular time in the payload. This is distance commitment on data payload and is illustrated in Figure 1.

Distance commitment assumes that channel state information (channel impulse response) is available after the SHR. The earliest path(s) are extracted from the channel state information available after the SHR is processed. During reception of PSDU only the “earliest path(s)” portion of the received signal shall be used for data decoding. Distance commitment ensures that the data of the PSDU carried by Challenge IE and Response IE is decoded at the measured distance by the earliest path(s).



Figure 1 Distance commitment principle and RF integration window

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 [B26]. 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 strictly defined by:

Δdmax = c0∙Tint,RF,

where c0 is the speed of light and processing delay equal to zero [B26]

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. Note that any other PHY with sufficiently short active RF duration can 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 | 14 cm – 75 cm |
| 128 | 1/2^128 (2.93e-39)  | MIC-128 | 14 cm – 75 cm |

**G.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 and is described in detail in section 3.1 [B28].