ICS 35.240.01
CCS L 70

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 47520-2026

Information technology - Real-time location systems - Ultra-wideband location air interface protocol

信息技术 实时定位系统 超宽带定位空中接口协议

Issued on: April 30, 2026 **Implemented on: November 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

5 General Principles

The air interface protocol in this document adopts a layered modular design, which is divided into a physical layer and a MAC layer. The physical layer adopts the UWB physical layer of IEEE 802.15.4.2020 and complies with the technical requirements and applicable laws of the national radio management agency. The scope was limited by the requirements of the scenario. The MAC layer protocol consists of a communication part (also known as the "communication protocol") and a positioning part (also known as the "positioning protocol"), as illustrated in Figure 1. As shown. The communication protocol defines operations such as base station broadcast beacons, tag and base station discovery, access, and periodic communication. The positioning protocol is used to implement... The protocol for UWB positioning-related functions is responsible for positioning measurements such as uplink TDoA, downlink TDoA, ToF, and AoA between the tag and the base station. operate. When the system does not support connectionless positioning, there is a dependency between the communication protocol and the positioning protocol at the tag end; the tag completes the communication first. After system authentication, the positioning protocol is executed. When the system supports connectionless positioning, the communication protocol and the positioning protocol communicate with each other between the tag and the base station. There are no dependencies on the site, and the tag can directly run the location protocol. The system's communication protocol and positioning protocol can share a single physical channel or use two separate physical channels.

6 Physical Layer

6.1 General Requirements It should comply with the requirements of IEEE 802.15.4z.2020, section 15.1.

6.2 Frame Format It should comply with the provisions of IEEE 802.15.4z.2020, section

15.2 and IEEE 802.15.4.2020, section 15.2. The key parameters used in this document are indexed as follows:

a) Number of PRF and preamble symbols. Should comply with the requirements of IEEE 802.15.4.2020, section 15.2.5;

b) Preamble index. It shall conform to the requirements of

15.2.6.2 in IEEE 802.15.4.2020;

c) SFD sequence. shall comply with the requirements of

15.2.6.3 in IEEE 802.15.4z.2020;

d) Data rate. It shall comply with the requirements of

15.2.4 in IEEE 802.15.4.2020.

6.3 Modulation It should comply with the requirements of

15.3 in IEEE 802.15.4z.2020.

6.4 Radio Frequency Requirements It should comply with the requirements of IEEE 802.15.4z.2020, section 15.4.RF-related specifications should meet the following requirements.

a) Operating frequency. 7163MHz~8812MHz.

7.3 Access Authentication and Data Encryption

7.3.1 General Requirements Access authentication and encrypted data transmission are enabled through MAC layer attribute configuration, see section 7.6.The authentication and encryption scheme adopts... The AES-CCM encryption algorithm is described in Chapter 9 of IEEE 802.15.4z.2020.

7.3.2 Access Authentication When a tag accesses the system, it sends an access request (see 8.3.1). The ASSOU frame (see 8.3) should carry an access authentication field. The access authentication field packet... The encrypted message contains the tag's long address and encrypted verification information. After receiving the access authentication field, the base station decrypts and verifies the encrypted information, checking if it matches the tag's address. If the signature and address match, and the encryption verification passes and the long address matches the tag, authentication is successful; otherwise, authentication fails. If the base station and tag... If the key does not match, the encryption field, or the encryption verification is modified, decryption will fail, access authentication will fail, and the base station will reply with the Asso-Conf tag. The base station status is "Label access authentication failed".

7.3.3 Encryption of Communication and Positioning Protocols Communication data frames and location data frames at the MAC layer can be encrypted independently. The frame

control field of the frame protocol marks the data frames as separate entities. Whether encryption is enabled for the location frame. The interaction flow between the authentication and encryption mechanisms of the communication and location protocol is shown in Figure

2.The darker part in the figure represents the communication. The encryption range in the protocol corresponds to the encryption field in the frame protocol format (the information field marked with an asterisk in the frame protocol format). The location protocol's encryption... The secret range refers to the information fields marked with an asterisk (*) in the location frame format protocol. The sending end encrypts the data before sending it, adding an encryption check field to the end of the data frame. The receiving end should decrypt the data upon receiving it. The encryption is checked for validity, and after successful decryption, the data packet is decrypted according to the protocol. If the base station and tag keys do not match, or the encryption key is incorrect... If the segment or encryption verification is modified, decryption will fail, normal communication will be impossible, and the receiving end will ignore the process.

7.4 Safe Distance Measurement STS secure ranging can be configured and enabled via MAC layer attributes. See section

7.6 for the secure ranging function, and the relevant solution is found in IEEE 802.15.4z. Section

15.2.9 of 2020 states that if STS secure ranging is enabled, all positioning protocol frames at the MAC layer should be configured to enable secure ranging according to the STS settings. The STS configuration scope does not include communication protocol frames. The encryption algorithm parameters are as follows:

a) The STS key is the same as the key in 7.3.3c);

b) The STSV length is 16 bytes. The initial value of each frame is fixed as all zeros. The protocol is generated within the frame according to the standard physical layer STS. The proposal was generated;

c) STS configuration is described in 7.7.2e).

7.5 Data Processing The storage and transmission of data in the data items defined in this document shall comply with the following rules.

a) For data formats arranged horizontally, data items are operated sequentially from left to right. For data formats arranged vertically, data items are operated sequentially from left to right. Operations in top-to-bottom order;

b) The byte order and bit order of data operations in the data item are processed in little-endian and least significant bit first manner. Note

1.Little-endian means that in data longer than one byte, the least significant byte is stored at a lower memory address or is transmitted first. Note

7.7 Extended Data

7.7.1 Extended Data Packet Format Extended data packets are additional information in MAC layer communication protocol frames, using a unified format. The format of extended data packets should conform to the requirements in Table 9. Request. Should extended data packets support the continuous transmission of multiple extended data packets (continuously concatenated data packets)?

7.7.2 Extended Packet Definition Each data type corresponds to a command word, and the data type name, data length, and data segment content should conform to the requirements of Table 10. 8.MAC Layer Air Interface Protocol

8.1 General Requirements for Communication Protocols Figure 3 illustrates the interaction between the tag and the base station communication frames, including enabling and disabling communication functions in the base station configuration. Figure

3.Schematic diagram of communication frame interaction between the tag and the base station (active scanning) Tag-based base station discovery can be achieved through two methods. passive scanning and active scanning. Passive scanning involves the tag activating its receiver to receive signals transmitted by the base station. For superframes, the scan reception duration should be greater than the superframe period; active scanning involves the tag actively sending scan frames, which the base station then receives. The tag replies with a Scan-Conf frame. Based on the received Scan-Conf result, the tag selects a base station to connect to. After a successful connection, it obtains the current system information. Related configuration. When the tag is connected, it periodically locates and communicates with the base station. The tag periodically uploads its current configuration and operating status. Complete uplink and downlink communication; the communication content includes extended data packets. In addition to Scan and Scan-Conf, communication between the tag and the base station should use either Conf or Ack acknowledgment mechanisms. When receiving the Ack,... The length is defined by the MAC layer attributes; see section

7.6 for the UWB response timeout function.

8.2 Active Scanning

8.2.1 General Requirements Tag-initiated scanning refers to a tag sending a Scan frame at any time and then entering receive mode. The duration of reception is determined by the MAC layer. Attribute definition (see

7.6 Function Tag Scan Receive Duration), default 10ms; the base station should return Scan-Conf to the tag upon receiving the Scan signal. The frames are sent with a uniformly random distribution and a delay. The tag selects a base station based on the RSSI and Scan-Conf information of all base stations. The selection strategy is defined by the tag itself,