TRANSMISSION METHOD, SYSTEM, AND RELATED APPARATUS

[0001] This application claims priority to Chinese Patent Application No. 202110878362.0, filed with the China National Intellectual Property Administration on July 31, 2021 and entitled "SECURE TRANSMISSION SOLUTION", and to Chinese Patent Application No. 202111166937.2, filed with the China National Intellectual Property Administration on September 30, 2021 and entitled "TRANSMISSION METHOD, SYSTEM, AND RELATED APPARATUS", which are incorporated herein by reference in their entireties.

[0002]

TECHNICAL FIELD

[0003] This application relates to the field of satellite communication, and in particular, to a transmission method, a system, and a related apparatus.

BACKGROUND

[0004] A satellite communication service may be used for positioning and communication in areas where mobile communication is unavailable or cannot be implemented, or where a communication system is damaged, such as oceans, deserts, grasslands, or uninhabited areas. At present, a satellite communication system does not provide civil terminals with a secure transmission mechanism for use. To securely transmit data between a terminal and a satellite, a communication protocol needs to be designed specific for civil service and device features and features of the satellite communication system.

[0005] Although there is a mature secure transmission mechanism in a cellular network, steps of the secure transmission mechanism in the cellular network are complex, and a large quantity of air interface resources are required for signaling exchange. The satellite communication system cannot support the secure transmission mechanism in the cellular network due to a long delay and limited air interface resources.

SUMMARY

[0006] This application discloses a transmission method, a system, and a related apparatus. A sending device may generate an authentication code A based on information A and original data. The sending device may send, to a receiving device in a first transmission system, a data packet including the authentication code A. After receiving the data packet, the receiving device may generate an authentication code B based on information B and the data packet. The receiving device may determine a receiving status of the data packet based on the authentication code B. The information A is sending time information and the information B is receiving time information, or the information A is context information A and the information B is context information B. In this way, after the receiving device receives a repeatedly sent data packet, the receiving device cannot parse the data packet, so that problems of repeated processing and charging do not occur.

[0007] According to a first aspect, this application provides a transmission method, including: a first device generates a first authentication code based on first information, a first key, and first data, where the first information is sending time information or first context information; the first device generates a first data packet based on the first authentication code and the first data; and the first device sends the first data packet to a second device in a first transmission system.

[0008] In a possible implementation, before the first device generates the first authentication code based on the first information, the first key, and the first data, the method further includes: the first device obtains the first key, where the first key is obtained by the first device through negotiation with the second device in a second transmission system, and the first transmission system is different from the second transmission system.

[0009] In a possible implementation, before the first device generates the first authentication code based on the first information, the first key, and the first data, the method further includes: the first device establishes a communication connection to a fourth device; and the first device obtains the first key through the fourth device.

[0010] In a possible implementation, the first key is a key preset by the first device.

[0011] In a possible implementation, the second transmission system is a cellular transmission system or a wireless local area network WLAN transmission system, and the first transmission system is a satellite transmission system.

[0012] In a possible implementation, the first device obtains the first key by negotiating with the second device by using a generic bootstrapping architecture GBA procedure in the second transmission system.

[0013] In a possible implementation, that the first device sends the first data packet to a second device in a first transmission system specifically includes:

after processing the first data packet into at least one second data packet at a message data convergence protocol MDCP layer of the first device and/or a satellite link control SLC layer of the first device, sending the at least one second data packet to the second device through a third device.

[0014] In a possible implementation, the sending time information indicates time at which the first device sends the first data packet.

[0015] In a possible implementation, the time at which the first device sends the first data packet is time at which an application AP layer of the first device sends the first data packet to the message data convergence protocol MDCP layer, or is time estimated by the first device for sending the first data packet to the second device.

[0016] In a possible implementation, the first device obtains the sending time information through positioning timing.

[0017] In a possible implementation, the first data packet includes packaged first data and the first authentication code.

[0018] In a possible implementation, a format of sending time of a data packet is universal time coordinated UTC or Greenwich mean time GMT.

[0019] In a possible implementation, a specified time granularity of the sending time of the data packet includes any one of a year, a month, a day, an hour, a minute, or a second. The first device and the second device update the specified time granularity through negotiation in the second transmission system.

[0020] In a possible implementation, the first device obtains the sending time information through the fourth device.

[0021] In a possible implementation, the first device obtains the first information based on the sending time information and a specified time granularity in a preset coding manner.

[0022] In a possible implementation, after the first device sends the first data packet, the method further includes:

the first device receives a first application layer receipt sent by the second device, where the first application layer receipt indicates a status of receiving the first data packet by the second device.

[0023] In a possible implementation, the first information is the first context information, and the first context information indicates information about a quantity of first data packets successfully sent by the first device, information about a quantity of application receipts successfully received by the first device, or a count value or a sequence number of the first data packet sent by the first device.

[0024] In a possible implementation, the first data packet further includes first indication

information, and the first indication information indicates a first message ID of the first data packet, or the first indication information indicates a first count value or a first sequence number of the first data packet.

[0025] In a possible implementation, an AP layer of the first device associates the first message ID, the first count value, or the first sequence number with the first data packet, and the first device adds a preset value to a value of the first message ID, the first count value, or the first sequence number.

[0026] In a possible implementation, the first data packet further includes third indication information, and the third indication information indicates that the first data packet is a newly transmitted data packet or a retransmitted data packet.

[0027] In a possible implementation, when a value of the third indication information is a first value, the third indication information indicates that the first data packet is a newly transmitted data packet; or when a value of the third indication information is a second value, the third indication information indicates that the first data packet is a retransmitted data packet.

[0028] In a possible implementation, before the first device generates the first authentication code based on the first information, the first key, and the first data, the method further includes:

the first device obtains an initial value of the first information in the second transmission system; or

the first device obtains an initial value of the first information through the fourth device.

[0029] In a possible implementation, after the first device sends the first data packet, the method further includes:

the first device receives a first application layer receipt sent by the second device, where the first application layer receipt indicates a status of receiving the first data packet by the second device.

[0030] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes:

the first device adds a preset value to a value of the first information, where an adjusted value of the first information is different from the value of the first information.

[0031] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt indicates that the second device fails to receive the first data packet, the first device adjusts the value of the first information to the initial value.

[0032] In a possible implementation, after the first device adjusts the value of the first information to the initial value, the method further includes: the first device sends third information to the second device, where a value of the third information is the same as the adjusted value of

the first information.

[0033] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt indicates that the first data packet is successfully sent, the first device displays success prompt information, where the success prompt information prompts a user that a message corresponding to the first data packet is successfully sent.

[0034] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt indicates that the first data packet fails to be sent, the first device displays failure prompt information, where the failure prompt information prompts a user that a message corresponding to the first data packet fails to be sent.

[0035] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt includes second message ID information, the first device displays success prompt information, where the success prompt information prompts a user that a data packet indicated by the second message ID information is successfully sent.

[0036] In a possible implementation, that the application layer of the first device generates a first data packet based on the first authentication code and the first data specifically includes: the application layer of the first device encrypts the first authentication code and the first data based on the first key, to generate the first data packet, where the first data packet includes an encrypted first authentication code and encrypted first data.

[0037] In a possible implementation, the application layer of the first device encrypts the first data based on the first key, to generate the first data packet, where the first data packet includes encrypted first data.

[0038] In a possible implementation, after the first device sends the first data packet to the second device in the first transmission system, the method further includes: the first device receives second application receipt information in the second transmission system, where the second application receipt information indicates a status of sending the first data packet by the first device in the first transmission system.

[0039] In a possible implementation, after the first device sends the first data packet to the second device in the first transmission system, the method further includes: the first device displays sending prompt information, where the sending prompt information prompts the user that the first device has sent the first data packet to the second device.

[0040] According to a second aspect, this application provides a transmission method, including: a second device receives, in a first transmission system, a first data packet sent by a first

device; the second device generates a second authentication code based on second information, a first key, and the first data packet, where the second information is receiving time information or second context information; and the second device determines a receiving status of the first data packet based on the second authentication code.

[0041] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device obtains the first key, where the first key is obtained by the second device through negotiation with the first device in a second transmission system, and the second transmission system is different from the first transmission system.

[0042] In a possible implementation, the second transmission system is a cellular transmission system or a WLAN transmission system, and the first transmission system is a satellite transmission system.

[0043] In a possible implementation, the second device obtains the first key by negotiating with the first device by using a generic bootstrapping architecture GBA procedure in the second transmission system.

[0044] In a possible implementation, the first key is a key preset by the first device.

[0045] In a possible implementation, that a second device receives a first data packet in a first transmission system specifically includes: the second device receives, in the first transmission system, the first data packet sent by a third device.

[0046] In a possible implementation, the second device determines a first authentication code based on the first data packet.

[0047] In a possible implementation, the receiving time information indicates receiving time of the first data packet.

[0048] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device receives the second information sent by the third device.

[0049] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device receives third information sent by the third device; and the second device generates the second information based on the third information.

[0050] In a possible implementation, the second context information indicates information about a quantity of first data packets successfully received by the second device, or a count value or a sequence value of the first data packet received by the second device.

[0051] In a possible implementation, the first data packet includes first indication information, and the first indication information indicates a first message ID/a first sequence number/a first

count value of the first data packet.

[0052] In a possible implementation, the first data packet includes third indication information, and the third indication information indicates that the first data packet is a newly transmitted data packet/a retransmitted data packet.

[0053] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device obtains an initial value of the second information in the second transmission system.

[0054] In a possible implementation, that the second device determines a receiving status of the first data packet based on the second authentication code specifically includes: the second device determines the receiving status of the first data packet based on whether the first authentication code is the same as the second authentication code.

[0055] In a possible implementation, that the second device compares the first authentication code with the second authentication code specifically includes: when the first authentication code is the same as the second authentication code, the second device determines that the first data packet is successfully received;

when the first authentication code is different from the second authentication code, the second device determines that the first data packet fails to be received; or

when the first authentication code is different from the second authentication code, the second device updates the second information and generates an updated second authentication code based on updated second information, and the second device compares the updated second authentication code with the first authentication code to determine the receiving status of the first data packet.

[0056] In a possible implementation, when the updated second authentication code is the same as the first authentication code, the second device determines that the first data packet is successfully received, and the second device adds a preset value to a value of the updated second information.

[0057] In a possible implementation, when the updated second authentication code is the same as the first authentication code, the second device generates and sends, to the first device, a first application receipt including second indication information, where the second indication information indicates a message ID of a latest successfully received data packet.

[0058] In a possible implementation, when the updated second authentication code is the same as the first authentication code, the second device generates and sends, to the first device, a first application receipt indicating that the first data packet is successfully sent.

[0059] In a possible implementation, when the updated second authentication code is different

from the first authentication code, the second device generates and sends, to the first device, a first application receipt indicating that the first data packet fails to be received.

[0060] In a possible implementation, that the second device compares the first authentication code with the second authentication code specifically includes: when the first authentication code is the same as the second authentication code, the second device determines that the first data packet is successfully received;

when the first authentication code is different from the second authentication code, the second device determines that the first data packet fails to be received; or

when the first authentication code is different from the second authentication code, the second device updates the second information and generates a temporary authentication code based on updated second information, and the second device compares the temporary authentication code with the first authentication code to determine the receiving status of the first data packet.

[0061] When the temporary authentication code is the same as the first authentication code, the second device generates and sends, to the first device, a first application receipt including second indication information, where the second indication information indicates a message ID of a latest successfully received data packet; or when the temporary authentication code is different from the first authentication code, the second device generates and sends, to the first device, a first application receipt indicating that the first data packet fails to be received.

[0062] In a possible implementation, after the second device determines that the first data packet is successfully received, the method further includes:

recording information about time at which the first data packet is successfully received;

recording a message ID corresponding to the first data packet; and/or

the second device adds a preset value to a value of the second information, where an adjusted value of the second information is different from the value of the second information.

[0063] In a possible implementation, that the second device compares the second authentication code with the first authentication code specifically includes: when the second authentication code is the same as the first authentication code, the second device determines that the first data packet is successfully received, and generates a first application layer receipt indicating that the first data packet is successfully received; or when the second authentication code is different from the first authentication code, the second device determines that the first data packet fails to be received, and generates a first application layer receipt indicating that the first data packet fails to be received.

[0064] In a possible implementation, that the second device compares the second authentication code with the first authentication code specifically includes: when the second

authentication code is the same as the first authentication code, the second device determines that the first data packet fails to be received, and generates a first application layer receipt indicating that the first data packet fails to be received, where the first application layer receipt includes a message ID corresponding to a successfully received data packet; or when the second authentication code is different from the first authentication code, the second device determines that the first data packet fails to be received, and generates a first application layer receipt indicating that the first data packet fails to be received.

[0065] In a possible implementation, after the second device determines the receiving status of the first data packet based on the second authentication code, the method further includes: when the second device determines, based on the second authentication code, that the first data packet is successfully received, the second device sends a first application receipt to the first device, where the first application receipt indicates that the first data packet is successfully received.

[0066] In a possible implementation, after the second device determines the receiving status of the first data packet based on the second authentication code, the method further includes: when the second device determines, based on the second authentication code, that the first data packet fails to be received, the second device sends a first application receipt to the first device, where the first application receipt further includes a second message ID, and the second message ID indicates a message ID corresponding to a latest successfully transmitted data packet.

[0067] In a possible implementation, after the second device determines the receiving status of the first data packet based on the second authentication code, the method further includes: when the second device determines, based on the second authentication code, that the first data packet fails to be received, the second device sends a first application receipt to the first device, where the first application receipt indicates that the first data packet fails to be received.

[0068] In a possible implementation, when the second device determines, based on the second authentication code, that the first data packet is successfully received, the method further includes: the second device adds a preset value to a value of the second information, where an adjusted value of the second information is different from the value of the second information.

[0069] In a possible implementation, when the second device determines, based on the second authentication code, that the first data packet fails to be received, the method further includes: the second device adjusts a value of the second information to a preset value.

[0070] In a possible implementation, when the second device determines, based on the second authentication code, that the first data packet fails to be received, the method further includes: the second device receives the third information sent by the first device; and the second device adjusts a value of the second information to a value of the third information.

[0071] In a possible implementation, after the second device determines the receiving status

of the first data packet based on the second authentication code, the method further includes: the second device sends second application receipt information to the first device in the second transmission system, where the second application receipt information indicates a status of receiving the first data packet by the second device in the first transmission system.

[0072] According to a third aspect, this application provides a transmission method, including:

a third device receives at least one second data packet sent by a first device;

the third device generates a first data packet based on the at least one second data packet; and

the third device sends the first data packet to a second device.

[0073] In a possible implementation, the third device sends second information or fourth information to the second device, where the second information or the fourth information is receiving time information.

[0074] In a possible implementation, the receiving time information indicates corresponding time at which the third device receives the 1st data packet in the at least one second data packet.

[0075] According to a fourth aspect, this application provides a transmission method, including:

a first device receives a third data packet in a first transmission system; and

the first device generates a third authentication code based on fifth information and the third data packet, where the fifth information is receiving time information or fifth context information; and the first device determines a receiving status of the third data packet based on the third authentication code.

[0076] In a possible implementation, that the first device generates a third authentication code based on fifth information and the third data packet specifically includes: the first device generates the third authentication code based on the fifth information, the third data packet, and a first key.

[0077] In a possible implementation, before the first device generates the third authentication code based on the fifth information, the first key, and the third data packet, the method further includes: the first device obtains the first key, where the first key is obtained by the first device through negotiation with a second device in a second transmission system, and the first transmission system is different from the second transmission system.

[0078] In a possible implementation, before the first device generates the third authentication code based on the fifth information, the first key, and the third data packet, the method further includes: the first device establishes a communication connection to a fourth device; and the first device obtains the first key through the fourth device.

[0079] In a possible implementation, the first key is a key preset by the first device.

[0080] In a possible implementation, the first transmission system is a satellite transmission

system, and the second transmission system is a non-satellite transmission system.

[0081] In a possible implementation, the second transmission system is a cellular transmission system or a wireless local area network WLAN transmission system.

[0082] In a possible implementation, the first device obtains the first key by negotiating with the second device by using a generic bootstrapping architecture (Generic Bootstrapping Architecture, GBA) procedure in the second transmission system.

[0083] In a possible implementation, the first device determines a fourth authentication code based on the third data packet.

[0084] In a possible implementation, that a first device receives a third data packet in a first transmission system specifically includes: the first device receives at least one fourth data packet sent by a third device; and a satellite link control SLC layer of the first device and/or a message data convergence protocol MDCP layer of the first device process/processes the at least one fourth data packet into the third data packet.

[0085] In a possible implementation, the fifth information is the receiving time information.

[0086] In a possible implementation, the receiving time information indicates time at which the first device receives the third data packet.

[0087] In a possible implementation, the time at which the first device receives the third data packet is time at which the first device receives the 1st fourth data packet in the at least one fourth data packet.

[0088] In a possible implementation, the first device obtains the fifth information through positioning timing.

[0089] In a possible implementation, the first device obtains the fifth information based on the receiving time information and a specified time granularity in a preset coding manner.

[0090] In a possible implementation, the fifth information is the fifth context information, and the fifth context information indicates information about a quantity of third data packets successfully received by the first device, or a count value or a sequence number of the third data packet received by the first device.

[0091] In a possible implementation, the third data packet includes sixth indication information, and the sixth indication information indicates a fourth message ID/a fourth sequence number/a fourth count value of the third data packet.

[0092] In a possible implementation, the third data packet includes fourth indication information, and the fourth indication information indicates that the third data packet is a newly transmitted data packet or a retransmitted data packet.

[0093] In a possible implementation, before the first device generates the third authentication code based on the fifth information, the first key, and the third data packet, the method further

includes: the first device obtains an initial value of the fifth information in the second transmission system.

[0094] In a possible implementation, that the first device determines a receiving status of the third data packet based on the third authentication code specifically includes: the first device determines the receiving status of the third data packet based on whether the third authentication code is the same as the fourth authentication code.

[0095] In a possible implementation, that the first device determines the receiving status of the third data packet based on whether the third authentication code is the same as the fourth authentication code specifically includes:

when the third authentication code is the same as the fourth authentication code, the first device determines that the third data packet is successfully received;

when the third authentication code is different from the fourth authentication code, the first device determines that the third data packet fails to be received; or

when the third authentication code is different from the fourth authentication code, the first device generates temporary information based on the fifth information and generates a temporary authentication code based on the temporary information, and the first device compares the fourth authentication code with the temporary authentication code to determine the receiving status of the third data packet.

[0096] When the fourth authentication code is the same as the temporary authentication code, the first device generates and sends, to the second device, a third application receipt including fifth indication information; or when the fourth authentication code is different from the temporary authentication code, the first device generates and sends, to the second device, a failure application receipt.

[0097] In a possible implementation, when the third authentication code is different from the fourth authentication code, the first device updates a value of the fifth information and generates an updated third authentication code based on updated fifth information, and the first device compares the updated third authentication code with the fourth authentication code to determine the receiving status of the third data packet.

[0098] In a possible implementation, when the updated third authentication code is the same as the fourth authentication code, the first device generates and sends, to the second device, a third application receipt including fifth indication information; or when the updated third authentication code is different from the fourth authentication code, the first device generates and sends, to the second device, a third application receipt indicating that the third data packet fails to be sent.

[0099] In a possible implementation, when the updated third authentication code is the same as the fourth authentication code, the first device generates and sends, to the second device, a third

application receipt indicating that the third data packet is successfully sent.

[00100] In a possible implementation, when the updated third authentication code is the same as the fourth authentication code, the first device adds a preset value to a value of the updated fifth information.

[00101] In a possible implementation, an indication application receipt includes the fifth indication information, and a value of the fifth indication information is the same as a value of sixth indication information of a latest successfully received data packet.

[00102] In a possible implementation, after the first device determines that the third data packet is successfully received, the method further includes:

recording information about time at which the third data packet is successfully received;

recording a message ID corresponding to the third data packet; and/or

adding a preset value to a value of the fifth information, where an adjusted value of the fifth information is different from the value of the fifth information.

[00103] In a possible implementation, after the first device determines the receiving status of the third data packet based on the third authentication code, the method further includes: the first device sends a third application receipt to the second device, where the third application receipt indicates the receiving status of the third data packet.

[00104] In a possible implementation, after the first device determines the receiving status of the third data packet based on the third authentication code, the method further includes: when the first device determines that the receiving status of the third data packet is correct receiving, the first device adds a preset value to a value of the fifth information, where an adjusted value of the fifth information is different from the value of the fifth information.

[00105] In a possible implementation, after the first device determines the receiving status of the third data packet based on the third authentication code, the method further includes: when the first device determines that the receiving status of the third data packet is failed receiving, the first device updates a value of the fifth information to a preset value. Optionally, the preset value is the initial value.

[00106] In a possible implementation, the method further includes: the first device receives seventh information sent by the second device; and the first device updates the value of the fifth information to a value of the seventh information based on the seventh information.

[00107] In a possible implementation, after the first device determines that the third data packet is successfully received, the method further includes: the first device displays third data.

[00108] In a possible implementation, after the first device determines the receiving status of the third data packet based on the third authentication code, the method further includes:

the first device sends third application receipt information to the second device in the

second transmission system, where the third application receipt information indicates a status of receiving the third data packet by the first device in the first transmission system.

[00109] According to a fifth aspect, this application provides a transmission method, including: a second device generates a fourth authentication code based on sixth information and third data, where the sixth information is sending time information or sixth context information; an application AP layer of the second device generates a third data packet based on the fourth authentication code and the first data; and the second device sends the third data packet to a first device in a first transmission system.

[00110] In a possible implementation, that a second device generates a fourth authentication code based on sixth information and first data specifically includes: the second device generates the fourth authentication code based on the sixth information, a first key, and the first data.

[00111] In a possible implementation, before the second device generates the fourth authentication code based on the sixth information, the first key, and the first data, the method further includes:

the second device obtains the first key, where the first key is obtained by the first device through negotiation with the second device in a second transmission system, and the first transmission system is different from the second transmission system.

[00112] In a possible implementation, the first key is a preset key.

[00113] In a possible implementation, the second device obtains the first key by negotiating with the first device by using a generic bootstrapping architecture (Generic Bootstrapping Architecture, GBA) procedure in the second transmission system.

[00114] In a possible implementation, that the second device sends the third data packet to a first device in a first transmission system specifically includes: the second device sends the third data packet to the first device through a third device.

[00115] In a possible implementation, the sixth information indicates the sending time information.

[00116] In a possible implementation, the sending time information indicates time at which the fourth authentication code is generated or time at which the second device sends the third data packet.

[00117] In a possible implementation, the time at which the second device sends the third data packet is time at which the second device delivers the third data packet to the third device, or is time estimated by the second device for sending the third data packet to the first device.

[00118] In a possible implementation, after obtaining the third data packet through packaging, the second device adds the fourth authentication code to the third data packet.

[00119] In a possible implementation, a format of the generation time of the fourth

authentication code is universal time coordinated UTC or Greenwich mean time GMT.

[00120] In a possible implementation, a minimum time granularity of the generation time of the fourth authentication code includes any one of a year, a month, a day, an hour, a minute, or a second.

[00121] In a possible implementation, the second device obtains the sixth information based on the sending time information and a specified time granularity in a specified encoding manner.

[00122] In a possible implementation, before the second device generates the fourth authentication code based on the sixth information, the first key, and the first data, the method further includes: the second device obtains the sixth information through the third device.

[00123] In a possible implementation, before the second device generates the fourth authentication code based on the sixth information, the first key, and the first data, the method further includes: the second device receives eighth information sent by the third device; and the second device generates the sixth information based on the eighth information.

[00124] Optionally, the second device receives the sixth information sent by the third device.

[00125] In a possible implementation, the sixth information is the sixth context information, and the sixth context information indicates information about a quantity of third data packets successfully sent by the second device, information about a quantity of application receipts successfully received by the second device, or a count value or a sequence value of the third data packet sent by the second device.

[00126] In a possible implementation, the method further includes: the second device obtains an initial value of the sixth information in the second transmission system; or the second device resets the sixth information to a preset value in the second transmission system.

[00127] In a possible implementation, the third data packet further includes sixth indication information, and the sixth indication information indicates a fourth message ID of the third data packet, or the sixth indication information indicates a fourth count value or a fourth sequence number of the third data packet.

[00128] In a possible implementation, when the sixth indication information indicates the fourth count value or the fourth sequence number of the third data packet, the method further includes: the application layer of the second device associates the fourth count value or the fourth sequence number with the third data packet, and the second device adds a preset value to a value of the fourth count value or the fourth sequence number.

[00129] In a possible implementation, the third data packet further includes fourth indication information, and the fourth indication information indicates new transmission/retransmission information of the third data packet.

[00130] In a possible implementation, that an application AP layer of the second device

generates a third data packet based on the fourth authentication code and the first data specifically includes: the application layer of the second device encrypts the fourth authentication code and the first data based on the first key, to generate the third data packet, where the third data packet includes an encrypted fourth authentication code and encrypted first data.

[00131] In a possible implementation, after the second device sends the third data packet, the method further includes:

the second device receives a third application layer receipt sent by the first device, where the third application layer receipt indicates a status of receiving the third data packet by the first device.

[00132] In a possible implementation, after the second device receives the third application layer receipt sent by the first device, the method further includes: the second device adds a preset value to a value of the sixth information, where an adjusted value of the sixth information is different from the value of the sixth information.

[00133] In a possible implementation, the second device receives fourth application receipt information in the second transmission system, where the fourth application receipt information indicates a status of sending the third data packet by the second device in the first transmission system; and

the second device updates a sending status based on the fourth application receipt information.

[00134] In a possible implementation, the second device deletes the successfully sent third data packet.

[00135] According to a sixth aspect, this application provides a transmission method, including:

a third device receives a third data packet sent by a second device;

the third device generates at least one fourth data packet based on the third data packet; and

the third device sends the at least one fourth data packet to a first device.

[00136] In a possible implementation, before the third device receives the third data packet sent by the second device, the method further includes: the third device sends second information or fourth information to the second device, where the second information or the fourth information is time information.

[00137] According to a seventh aspect, this application provides a transmission method, including:

a first device generates a first authentication code based on first information, a first key, and first data, where the first information is sending time information or first context information;

the first device generates a first data packet based on the first authentication code and the first data;

and the first device sends the first data packet to a second device in a first transmission system.

[00138] In a possible implementation, before the first device generates the first authentication code based on the first information, the first key, and the first data, the method further includes: the first device obtains the first key, where the first key is obtained by the first device through negotiation with the second device in a second transmission system, and the first transmission system is different from the second transmission system.

[00139] In a possible implementation, before the first device generates the first authentication code based on the first information, the first key, and the first data, the method further includes: the first device establishes a communication connection to a fourth device; and the first device obtains the first key through the fourth device.

[00140] In a possible implementation, the first key is a key preset by the first device.

[00141] In a possible implementation, the second transmission system is a cellular transmission system or a wireless local area network WLAN transmission system, and the first transmission system is a satellite transmission system.

[00142] In a possible implementation, the first device obtains the first key by negotiating with the second device by using a generic bootstrapping architecture GBA procedure in the second transmission system.

[00143] In a possible implementation, the sending time information indicates time at which the first authentication code is generated, or indicate time at which the first device sends the first data packet.

[00144] In a possible implementation, the time at which the first device sends the first data packet is time at which an application AP layer of the first device sends the first data packet to a message data convergence protocol MDCP layer, or is time estimated by the first device for sending the first data packet to the second device.

[00145] In a possible implementation, the first device obtains the sending time information through positioning timing.

[00146] In a possible implementation, the first data packet includes packaged first data and the first authentication code.

[00147] In a possible implementation, a format of sending time of a data packet is universal time coordinated UTC or Greenwich mean time GMT.

[00148] In a possible implementation, a specified time granularity of the sending time of the data packet includes any one of a year, a month, a day, an hour, a minute, or a second. The first device and the second device update the specified time granularity through negotiation in the second transmission system.

[00149] In a possible implementation, the first device obtains the sending time information

through the fourth device.

[00150] In a possible implementation, the first device obtains the first information based on the sending time information and a specified time granularity in a preset coding manner.

[00151] In a possible implementation, after the first device sends the first data packet, the method further includes:

the first device receives a first application layer receipt sent by the second device, where the first application layer receipt indicates a status of receiving the first data packet by the second device.

[00152] In a possible implementation, the first information is the first context information, and the first context information indicates information about a quantity of first data packets successfully sent by the first device, information about a quantity of application receipts successfully received by the first device, or a count value or a sequence number of the first data packet sent by the first device.

[00153] In a possible implementation, the first data packet further includes first indication information, and the first indication information indicates a first message ID of the first data packet, or the first indication information indicates a first count value or a first sequence number of the first data packet.

[00154] In a possible implementation, an AP layer of the first device associates the first message ID, the first count value, or the first sequence number with the first data packet, and the first device adds a preset value to a value of the first message ID, the first count value, or the first sequence number.

[00155] In a possible implementation, the first data packet further includes third indication information, and the third indication information indicates that the first data packet is a newly transmitted data packet or a retransmitted data packet.

[00156] In a possible implementation, when a value of the third indication information is a first value, the third indication information indicates that the first data packet is a newly transmitted data packet; or when a value of the third indication information is a second value, the third indication information indicates that the first data packet is a retransmitted data packet.

[00157] In a possible implementation, before the first device generates the first authentication code based on the first information, the first key, and the first data, the method further includes:

the first device obtains an initial value of the first information in the second transmission system; or

the first device obtains an initial value of the first information through the fourth device.

[00158] In a possible implementation, after the first device sends the first data packet, the method further includes:

the first device receives a first application layer receipt sent by the second device, where the first application layer receipt indicates a status of receiving the first data packet by the second device.

[00159] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes:

the first device adds a preset value to a value of the first information, where an adjusted value of the first information is different from the value of the first information.

[00160] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt indicates that the second device fails to receive the first data packet, the first device adjusts the value of the first information to the initial value.

[00161] In a possible implementation, after the first device adjusts the value of the first information to the initial value, the method further includes: the first device sends third information to the second device, where a value of the third information is the same as the adjusted value of the first information.

[00162] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt indicates that the first data packet is successfully sent, the first device displays success prompt information, where the success prompt information prompts a user that a message corresponding to the first data packet is successfully sent.

[00163] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt indicates that the first data packet fails to be sent, the first device displays failure prompt information, where the failure prompt information prompts a user that a message corresponding to the first data packet fails to be sent.

[00164] In a possible implementation, after the first device receives the first application layer receipt sent by the second device, the method further includes: when the first application receipt includes second message ID information, the first device displays success prompt information, where the success prompt information prompts a user that a data packet indicated by the second message ID information is successfully sent.

[00165] In a possible implementation, that the application layer of the first device generates a first data packet based on the first authentication code and the first data specifically includes: the application layer of the first device encrypts the first authentication code and the first data based on the first key, to generate the first data packet, where the first data packet includes an encrypted first authentication code and encrypted first data.

[00166] In a possible implementation, the application layer of the first device encrypts the first data based on the first key, to generate the first data packet, where the first data packet includes encrypted first data.

[00167] In a possible implementation, after the first device sends the first data packet to the second device in the first transmission system, the method further includes: the first device receives second application receipt information in the second transmission system, where the second application receipt information indicates a status of sending the first data packet by the first device in the first transmission system.

[00168] In a possible implementation, after the first device sends the first data packet to the second device in the first transmission system, the method further includes: the first device displays sending prompt information, where the sending prompt information prompts the user that the first device has sent the first data packet to the second device.

[00169] According to an eighth aspect, this application provides a transmission method, including: a second device receives, in a first transmission system, a first data packet sent by a first device; the second device generates a second authentication code based on second information, a first key, and the first data packet, where the second information is receiving time information or second context information; and the second device determines a receiving status of the first data packet based on the second authentication code.

[00170] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device obtains the first key, where the first key is obtained by the second device through negotiation with the first device in a second transmission system, and the second transmission system is different from the first transmission system.

[00171] In a possible implementation, the second transmission system is a cellular transmission system or a WLAN transmission system, and the first transmission system is a satellite transmission system.

[00172] In a possible implementation, the second device obtains the first key by negotiating with the first device by using a generic bootstrapping architecture GBA procedure in the second transmission system.

[00173] In a possible implementation, the first key is a key preset by the first device.

[00174] In a possible implementation, that a second device receives a first data packet in a first transmission system specifically includes: a satellite link control SLC layer of the second device receives at least one second data packet sent by the first device; and a message data convergence protocol MDCP layer of the second device and/or the satellite link control layer SLC layer of the second device obtain/obtains the first data packet based on the at least one second data packet.

[00175] In a possible implementation, the second device determines a first authentication code based on the first data packet.

[00176] In a possible implementation, the receiving time information indicates receiving time of the first data packet.

[00177] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device obtains the receiving time of the first data packet at the MDCP layer/the SLC layer; and the second device generates the second information based on the receiving time of the first data packet at the MDCP layer/the SLC layer.

[00178] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device obtains the receiving time of the first data packet at the MDCP layer/the SLC layer; the second device determines that the receiving time of the first data packet is eighth information, and uploads the eighth information to an AP layer; and the second device generates the second information based on the eighth information at the AP layer.

[00179] In a possible implementation, the second context information indicates information about a quantity of first data packets successfully received by the second device, or a count value or a sequence value of the first data packet received by the second device.

[00180] In a possible implementation, the first data packet includes first indication information, and the first indication information indicates a first message ID/a first sequence number/a first count value of the first data packet.

[00181] In a possible implementation, the first data packet includes third indication information, and the third indication information indicates that the first data packet is a newly transmitted data packet/a retransmitted data packet.

[00182] In a possible implementation, before the second device generates the second authentication code based on the second information, the first key, and the first data packet, the method further includes: the second device obtains an initial value of the second information in the second transmission system.

[00183] In a possible implementation, that the second device determines a receiving status of the first data packet based on the second authentication code specifically includes: the second device determines the receiving status of the first data packet based on whether the first authentication code is the same as the second authentication code.

[00184] In a possible implementation, that the second device compares the first authentication code with the second authentication code specifically includes: when the first authentication code is the same as the second authentication code, the second device determines that the first data

packet is successfully received;

when the first authentication code is different from the second authentication code, the second device determines that the first data packet fails to be received; or

when the first authentication code is different from the second authentication code, the second device updates the second information and generates a temporary authentication code based on updated second information, and the second device compares the temporary authentication code with the first authentication code to determine the receiving status of the first data packet.

[00185] When the temporary authentication code is the same as the first authentication code, the second device generates and sends, to the first device, a first application receipt including second indication information, where the second indication information indicates a message ID of a latest successfully received data packet; or when the temporary authentication code is different from the first authentication code, the second device generates and sends, to the first device, a first application receipt indicating that the first data packet fails to be received.

[00186] In a possible implementation, after the second device determines that the first data packet is successfully received, the method further includes:

recording information about time at which the first data packet is successfully received;

recording a message ID corresponding to the first data packet; and/or

the second device adds a preset value to a value of the second information, where an adjusted value of the second information is different from the value of the second information.

[00187] In a possible implementation, that the second device compares the second authentication code with the first authentication code specifically includes: when the second authentication code is the same as the first authentication code, the second device determines that the first data packet is successfully received, and generates a first application layer receipt indicating that the first data packet is successfully received; or when the second authentication code is different from the first authentication code, the second device determines that the first data packet fails to be received, and generates a first application layer receipt indicating that the first data packet fails to be received.

[00188] In a possible implementation, that the second device compares the second authentication code with the first authentication code specifically includes: when the second authentication code is the same as the first authentication code, the second device determines that the first data packet fails to be received, and generates a first application layer receipt indicating that the first data packet fails to be received, where the first application layer receipt includes a message ID corresponding to a successfully received data packet; or when the second authentication code is different from the first authentication code, the second device determines

that the first data packet fails to be received, and generates a first application layer receipt indicating that the first data packet fails to be received.

[00189] In a possible implementation, after the second device determines the receiving status of the first data packet based on the second authentication code, the method further includes: when the second device determines, based on the second authentication code, that the first data packet is successfully received, the second device sends a first application receipt to the first device, where the first application receipt indicates that the first data packet is successfully received.

[00190] In a possible implementation, after the second device determines the receiving status of the first data packet based on the second authentication code, the method further includes: when the second device determines, based on the second authentication code, that the first data packet fails to be received, the second device sends a first application receipt to the first device, where the first application receipt further includes a second message ID, and the second message ID indicates a message ID corresponding to a latest successfully transmitted data packet.

[00191] In a possible implementation, after the second device determines the receiving status of the first data packet based on the second authentication code, the method further includes: when the second device determines, based on the second authentication code, that the first data packet fails to be received, the second device sends a first application receipt to the first device, where the first application receipt indicates that the first data packet fails to be received.

[00192] In a possible implementation, when the second device determines, based on the second authentication code, that the first data packet is successfully received, the method further includes: the second device adds a preset value to a value of the second information, where an adjusted value of the second information is different from the value of the second information.

[00193] In a possible implementation, when the second device determines, based on the second authentication code, that the first data packet fails to be received, the method further includes: the second device adjusts a value of the second information to a preset value.

[00194] In a possible implementation, when the second device determines, based on the second authentication code, that the first data packet fails to be received, the method further includes: the second device receives third information sent by the first device; and the second device adjusts a value of the second information to a value of the third information.

[00195] In a possible implementation, after the second device determines the receiving status of the first data packet based on the second authentication code, the method further includes: the second device sends second application receipt information to the first device in the second transmission system, where the second application receipt information indicates a status of receiving the first data packet by the second device in the first transmission system.

[00196] According to a ninth aspect, this application provides a transmission method, including:

a first device receives a third data packet in a first transmission system; and

the first device generates a third authentication code based on fifth information and the third data packet, where the fifth information is sending time information or fifth context information; and the first device determines a receiving status of the third data packet based on the third authentication code.

[00197] In a possible implementation, that the first device generates a third authentication code based on fifth information and the third data packet specifically includes: the first device generates the third authentication code based on the fifth information, the third data packet, and a first key.

[00198] In a possible implementation, before the first device generates the third authentication code based on the fifth information, the first key, and the third data packet, the method further includes: the first device obtains the first key, where the first key is obtained by the first device through negotiation with a second device in a second transmission system, and the first transmission system is different from the second transmission system.

[00199] In a possible implementation, before the first device generates the third authentication code based on the fifth information, the first key, and the third data packet, the method further includes: the first device establishes a communication connection to a fourth device; and the first device obtains the first key through the fourth device.

[00200] In a possible implementation, the first key is a key preset by the first device.

[00201] In a possible implementation, the first transmission system is a satellite transmission system, and the second transmission system is a non-satellite transmission system.

[00202] In a possible implementation, the second transmission system is a cellular transmission system or a wireless local area network WLAN transmission system.

[00203] In a possible implementation, the first device obtains the first key by negotiating with the second device by using a generic bootstrapping architecture (Generic Bootstrapping Architecture, GBA) procedure in the second transmission system.

[00204] In a possible implementation, the first device determines a fourth authentication code based on the third data packet.

[00205] In a possible implementation, that a first device receives a third data packet in a first transmission system specifically includes: the first device receives at least one fourth data packet sent by the second device; and a satellite link control SLC layer of the first device and/or a message data convergence protocol MDCP layer of the first device process/processes the at least one fourth data packet into the third data packet.

[00206] In a possible implementation, the fifth information is the receiving time information.

[00207] In a possible implementation, the receiving time information indicates time at which the first device receives the third data packet.

[00208] In a possible implementation, the time at which the first device receives the third data packet is time at which the first device receives the 1st fourth data packet in the at least one fourth data packet.

[00209] In a possible implementation, the first device obtains the fifth information through positioning timing.

[00210] In a possible implementation, the first device obtains the fifth information based on the receiving time information and a specified time granularity in a preset coding manner.

[00211] In a possible implementation, the fifth information is the fifth context information, and the fifth context information indicates information about a quantity of third data packets successfully received by the first device, or a count value or a sequence number of the third data packet received by the first device.

[00212] In a possible implementation, the third data packet includes sixth indication information, and the sixth indication information indicates a fourth message ID/a fourth sequence number/a fourth count value of the third data packet.

[00213] In a possible implementation, the third data packet includes fourth indication information, and the fourth indication information indicates that the third data packet is a newly transmitted data packet or a retransmitted data packet.

[00214] In a possible implementation, before the first device generates the third authentication code based on the fifth information, the first key, and the third data packet, the method further includes: the first device obtains an initial value of the fifth information in the second transmission system.

[00215] In a possible implementation, that the first device determines a receiving status of the third data packet based on the third authentication code specifically includes: the first device determines the receiving status of the third data packet based on whether the third authentication code is the same as the fourth authentication code.

[00216] In a possible implementation, that the first device determines the receiving status of the third data packet based on whether the third authentication code is the same as the fourth authentication code specifically includes:

when the third authentication code is the same as the fourth authentication code, the first device determines that the third data packet is successfully received;

when the third authentication code is different from the fourth authentication code, the first device determines that the third data packet fails to be received; or

when the third authentication code is different from the fourth authentication code, the first device generates temporary information based on the fifth information and generates a temporary authentication code based on the temporary information, and the first device compares

the fourth authentication code with the temporary authentication code to determine the receiving status of the third data packet.

[00217] When the fourth authentication code is the same as the temporary authentication code, the first device generates and sends, to the second device, an indication application receipt; or when the fourth authentication code is different from the temporary authentication code, the first device generates and sends, to the second device, a failure application receipt.

[00218] In a possible implementation, the indication application receipt includes fifth indication information, and a value of the fifth indication information is the same as a value of sixth indication information of a latest successfully received data packet.

[00219] In a possible implementation, after the first device determines that the third data packet is successfully received, the method further includes:

recording information about time at which the third data packet is successfully received;

recording a message ID corresponding to the third data packet; and/or

adding a preset value to a value of the fifth information, where an adjusted value of the fifth information is different from the value of the fifth information.

[00220] In a possible implementation, after the first device determines the receiving status of the third data packet based on the third authentication code, the method further includes: the first device sends a third application receipt to the second device, where the third application receipt indicates the receiving status of the third data packet.

[00221] In a possible implementation, after the first device determines the receiving status of the third data packet based on the third authentication code, the method further includes: when the first device determines that the receiving status of the third data packet is correct receiving, the first device adds a preset value to a value of the fifth information, where an adjusted value of the fifth information is different from the value of the fifth information.

[00222] In a possible implementation, after the first device determines the receiving status of the third data packet based on the third authentication code, the method further includes: when the first device determines that the receiving status of the third data packet is failed receiving, the first device updates a value of the fifth information to a preset value. Optionally, the preset value is the initial value.

[00223] In a possible implementation, the method further includes: the first device receives seventh information sent by the second device; and the first device updates the value of the fifth information to a value of the seventh information based on the seventh information.

[00224] In a possible implementation, after the first device determines that the third data packet is successfully received, the method further includes: the first device displays third data.

[00225] In a possible implementation, after the first device determines the receiving status of

the third data packet based on the third authentication code, the method further includes:

the first device sends third application receipt information to the second device in the second transmission system, where the third application receipt information indicates a status of receiving the third data packet by the second device in the first transmission system.

[00226] According to a tenth aspect, this application provides a transmission method, including:

a second device generates a fourth authentication code based on sixth information and first data, where the sixth information is sending time information or sixth context information; an application AP layer of the second device generates a third data packet based on the fourth authentication code and the first data; and the second device sends the third data packet to a first device in a first transmission system.

[00227] In a possible implementation, that a second device generates a fourth authentication code based on sixth information and first data specifically includes: the second device generates the fourth authentication code based on the sixth information, a first key, and the first data.

[00228] In a possible implementation, before the second device generates the fourth authentication code based on the sixth information, the first key, and the first data, the method further includes:

the second device obtains the first key, where the first key is obtained by the first device through negotiation with the second device in a second transmission system, and the first transmission system is different from the second transmission system.

[00229] In a possible implementation, the first key is a preset key.

[00230] In a possible implementation, the second device obtains the first key by negotiating with the first device by using a generic bootstrapping architecture (Generic Bootstrapping Architecture, GBA) procedure in the second transmission system.

[00231] In a possible implementation, that the second device sends the third data packet to a first device in a first transmission system specifically includes: the second device sends the third data packet to the first device through a third device.

[00232] In a possible implementation, the sixth information indicates the sending time information.

[00233] In a possible implementation, the sending time information indicates time at which the fourth authentication code is generated or time at which the second device sends the third data packet.

[00234] In a possible implementation, the time at which the second device sends the third data packet is time at which the second device delivers the third data packet to the third device, or is time estimated by the second device for sending the third data packet to the first device.

[00235] In a possible implementation, after obtaining the third data packet through packaging,

the second device adds the fourth authentication code to the third data packet.

[00236] In a possible implementation, a format of the generation time of the fourth authentication code is universal time coordinated UTC or Greenwich mean time GMT.

[00237] In a possible implementation, a minimum time granularity of the generation time of the fourth authentication code includes any one of a year, a month, a day, an hour, a minute, or a second.

[00238] In a possible implementation, the second device obtains the sixth information based on the sending time information and a specified time granularity in a specified encoding manner.

[00239] In a possible implementation, before the second device generates the fourth authentication code based on the sixth information, the first key, and the first data, the method further includes: the second device obtains the sixth information through the third device.

[00240] In a possible implementation, before the second device generates the fourth authentication code based on the sixth information, the first key, and the first data, the method further includes: an MDCP layer/an SLC layer of the second device obtains eighth information; and the second device generates the sixth information based on the eighth information at the AP layer.

[00241] Optionally, the second device generates the sixth information at the MDCP layer/the SLC layer.

[00242] In a possible implementation, the sixth information is the sixth context information, and the sixth context information indicates information about a quantity of third data packets successfully sent by the second device, information about a quantity of application receipts successfully received by the second device, or a count value or a sequence value of the third data packet sent by the second device.

[00243] In a possible implementation, the method further includes: the second device obtains an initial value of the sixth information in the second transmission system; or the second device resets the sixth information to a preset value in the second transmission system.

[00244] In a possible implementation, the third data packet further includes sixth indication information, and the sixth indication information indicates a fourth message ID of the third data packet, or the sixth indication information indicates a fourth count value or a fourth sequence number of the third data packet.

[00245] In a possible implementation, when the sixth indication information indicates the fourth count value or the fourth sequence number of the third data packet, the method further includes: the application layer of the second device associates the fourth count value or the fourth sequence number with the third data packet, and the second device adds a preset value to a value of the fourth count value or the fourth sequence number.

[00246] In a possible implementation, the third data packet further includes fourth indication information, and the fourth indication information indicates new transmission/retransmission information of the third data packet.

[00247] In a possible implementation, that an application AP layer of the second device generates a third data packet based on the fourth authentication code and the first data specifically includes: the application layer of the second device encrypts the fourth authentication code and the first data based on the first key, to generate the third data packet, where the third data packet includes an encrypted fourth authentication code and encrypted first data.

[00248] In a possible implementation, after the second device sends the third data packet, the method further includes:

the second device receives a third application layer receipt sent by the first device, where the third application layer receipt indicates a status of receiving the third data packet by the first device.

[00249] In a possible implementation, after the second device receives the third application layer receipt sent by the first device, the method further includes: the second device adds a preset value to a value of the sixth information, where an adjusted value of the sixth information is different from the value of the sixth information.

[00250] In a possible implementation, the second device receives fourth application receipt information in the second transmission system, where the fourth application receipt information indicates a status of sending the third data packet by the second device in the first transmission system; and

the second device updates a sending status based on the fourth application receipt information.

[00251] In a possible implementation, the second device deletes the successfully sent third data packet.

[00252] According to an eleventh aspect, this application provides a transmission method, including:

a sending device generates an authentication code A based on information A and original data, where the information A is sending time information or context information A; the sending device obtains a data packet based on the authentication code A and the original data; and the sending device sends the data packet to a receiving device in a first transmission system.

[00253] In a possible implementation, that a sending device generates an authentication code A based on information A and original data specifically includes: the sending device generates the authentication code A based on the information A, a specified key, and the original data.

[00254] In a possible implementation, the sending device obtains the specified key by

negotiating with the receiving device in a second transmission system.

[00255] In a possible implementation, the first transmission system is different from the second transmission system.

[00256] In a possible implementation, the specified key is a key preset by the sending device.

[00257] In a possible implementation, the second transmission system is a cellular transmission system or a wireless local area network WLAN transmission system, and the first transmission system is a satellite transmission system.

[00258] In a possible implementation, the sending device obtains the specified key by negotiating with the receiving device by using a generic bootstrapping architecture GBA procedure in the second transmission system.

[00259] In a possible implementation, the information A is the sending time information, and the information A indicates sending time of the data packet.

[00260] In a possible implementation, time at which the sending device sends the data packet is time at which an application AP layer of the sending device sends the data packet to a message data convergence protocol MDCP layer, or is time estimated by the sending device for sending the data packet to the receiving device.

[00261] In a possible implementation, the information A is the context information A, and the information A indicates information about a quantity of sent data packets, or a sequence number or a count value of the data packet.

[00262] In a possible implementation, the data packet further includes a message ID field A, and the message ID field A is used to identify the data packet.

[00263] In a possible implementation, the data packet further includes a sequence number field A, and the sequence number field A is used to identify the data packet and further indicates the information A.

[00264] In a possible implementation, the sending device associates a sequence number A with the data packet, and generates the sequence number field A based on the sequence number A.

[00265] In a possible implementation, the sending device associates a message ID with the data packet, and generates the message ID field A based on the message ID.

[00266] In a possible implementation, the data packet further includes a retransmission indication field, and the retransmission indication field indicates that the data packet is a retransmitted data packet or a newly transmitted data packet.

[00267] In a possible implementation, the sending device encrypts the original data and the authentication code A by using the specified key, and then adds packet header information in front of encrypted original data and an encrypted authentication code A, to obtain the data packet. The packet header information includes an encryption indication field, and the encryption indication

field indicates an encryption algorithm used by the sending device.

[00268] In a possible implementation, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: the sending device adds a preset value to the sequence number A; and the sending device adjusts a value of the context information A based on an adjusted sequence number A.

[00269] In a possible implementation, that the sending device adjusts a value of the context information A based on an adjusted sequence number A specifically includes: the sending device determines a value of a hyper frame number A based on the adjusted sequence number A, and adjusts the value of the context information A based on the adjusted sequence number A and the hyper frame number A.

[00270] In a possible implementation, the sending device is a terminal, and the receiving device is a satellite network device.

[00271] In a possible implementation, the sending device is a satellite network device, and the receiving device is a terminal.

[00272] In a possible implementation, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after receiving a success application receipt sent by the receiving device, the sending device adds a preset value to a value of the context information A, where the success application receipt indicates that the receiving device successfully receives the data packet.

[00273] In a possible implementation, when the sending device is a terminal, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after the sending device receives the success application receipt sent by the receiving device, the sending device displays success prompt information, where the success prompt information prompts a user that the data packet is successfully sent.

[00274] In a possible implementation, when the sending device is a satellite network device, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after the sending device receives the success application receipt sent by the receiving device, the sending device deletes the data packet in a memory.

[00275] In a possible implementation, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after receiving a failure application receipt sent by the receiving device, the sending device adds a preset value to a value of the context information A, where the failure application receipt indicates that the receiving device fails to receive the data packet.

[00276] In a possible implementation, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after receiving a

failure application receipt sent by the receiving device, the sending device adjusts a value of the context information A to a preset value.

[00277] In a possible implementation, after the sending device adjusts the value of the context information A to the preset value, the method further includes: the sending device sends the value of the context information A to the receiving device.

[00278] In a possible implementation, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after the sending device receives a failure application receipt sent by the receiving device, the sending device negotiates with the receiving device about a value of the context information A in the second transmission system.

[00279] In a possible implementation, when the sending device is a terminal, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after the sending device receives the failure application receipt sent by the receiving device, the sending device displays failure prompt information, where the failure prompt information prompts a user that the data packet fails to be sent.

[00280] In a possible implementation, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after the sending device receives an indication application receipt sent by the receiving device, the sending device adds a preset value to a value of the context information A, where the indication application receipt indicates that the current data packet fails to be sent, the indication application receipt includes a message ID field B, and the message ID field B indicates a latest successfully sent data packet.

[00281] In a possible implementation, when the sending device is a terminal, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after the sending device receives the indication application receipt sent by the receiving device, the sending device displays success prompt information and failure prompt information, where the success prompt information prompts a user that the data packet indicated by the message ID field B is successfully sent, and the failure prompt information prompts the user that the current data packet fails to be sent.

[00282] In a possible implementation, when the sending device is a terminal, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: the sending device displays sending prompt information, where the sending prompt information prompts the user that the sending device has sent the data packet to the receiving device.

[00283] In a possible implementation, after the sending device sends the data packet to the receiving device in the first transmission system, the method further includes: after receiving, in

the second transmission system, a set application receipt sent by the receiving device, the sending device determines, based on the set application receipt, a receiving status of the data packet sent in the first transmission system.

[00284] According to a twelfth aspect, this application provides a transmission method, including: a receiving device receives, in a first transmission system, a data packet sent by a sending device; the receiving device generates an authentication code B based on information B and the data packet, where the information B is receiving time information or context information B; and the receiving device determines a receiving status of the data packet based on the authentication code B.

[00285] In a possible implementation, that the receiving device generates an authentication code B based on information B and original data specifically includes: the receiving device generates the authentication code B based on the information B, a specified key, and the original data.

[00286] In a possible implementation, the receiving device obtains the specified key by negotiating with the sending device in a second transmission system.

[00287] In a possible implementation, the first transmission system is different from the second transmission system.

[00288] In a possible implementation, the specified key is a key preset by the receiving device.

[00289] In a possible implementation, the second transmission system is a cellular transmission system or a wireless local area network WLAN transmission system, and the first transmission system is a satellite transmission system.

[00290] In a possible implementation, the receiving device obtains the specified key by negotiating with the sending device by using a generic bootstrapping architecture GBA procedure in the second transmission system.

[00291] In a possible implementation, the information B is the receiving time information, and the information B indicates receiving time of the data packet.

[00292] In a possible implementation, time at which the receiving device receives the data packet is time at which a satellite link control SLC layer of the receiving device receives the first satellite link control protocol data unit SLC PDU of the data packet.

[00293] In a possible implementation, the information B is the context information B, and the information B indicates information about a quantity of received data packets, or a sequence number or a count value of the data packet.

[00294] In a possible implementation, the data packet further includes a sequence number field A, and the sequence number field A is used to identify the data packet and further indicates the context information B.

[00295] In a possible implementation, the receiving device determines a value of the context

information B based on the sequence number field A and a stored sequence number B.

[00296] In a possible implementation, that the receiving device determines a value of the context information B based on the sequence number field A and a stored sequence number B specifically includes: the receiving device determines a value of a hyper frame number B based on the sequence number field A and a value of the sequence number B; and the receiving device obtains the context information B based on the sequence number field A and the hyper frame number B.

[00297] In a possible implementation, when a value of the sequence number field A is less than or equal to the value of the sequence number B, the receiving device adds a preset value to the value of the hyper frame number B.

[00298] In a possible implementation, the receiving device concatenates the hyper frame number B and the sequence number field A, to obtain the context information B.

[00299] In a possible implementation, after obtaining the context information B, the receiving device may adjust the value of the sequence number B to the value of the sequence number field A.

[00300] In a possible implementation, the data packet further includes a message ID field A, and the message ID field A is used to identify the data packet.

[00301] In a possible implementation, the receiving device is a satellite network device, and the sending device is a terminal.

[00302] In a possible implementation, the receiving device is a terminal, and the sending device is a satellite network device.

[00303] In a possible implementation, the receiving device obtains an authentication code A based on the data packet.

[00304] In a possible implementation, that the receiving device determines a receiving status of the data packet based on the authentication code B specifically includes: the receiving device compares the authentication code A with the authentication code B to determine the receiving status of the data packet.

[00305] In a possible implementation, that the receiving device compares the authentication code A with the authentication code B to determine the receiving status of the data packet specifically includes: when the authentication code B is the same as the authentication code A, the receiving device determines that the data packet is successfully received.

[00306] In a possible implementation, after the receiving device determines that the data packet is successfully received, the method further includes: the receiving device generates a success application receipt, where the success application receipt indicates that the receiving device successfully receives the data packet; and the receiving device sends the success application

receipt to the sending device.

[00307] In a possible implementation, the data packet includes the message ID field A; and after the receiving device determines that the data packet is successfully received, the method further includes: the receiving device adjusts a value of a message ID field B to a value of the message ID field A.

[00308] In a possible implementation, when the receiving device is a terminal, after the receiving device determines that the data packet is successfully received, the method further includes: the receiving device displays the original data.

[00309] In a possible implementation, when the receiving device is a satellite network device, after the receiving device determines that the data packet is successfully received, the method further includes: the receiving device sends the original data to an electronic device in the second transmission system through the second transmission system.

[00310] In a possible implementation, that the receiving device compares the authentication code A with the authentication code B to determine the receiving status of the data packet specifically includes: when the authentication code B is different from the authentication code A, the receiving device determines that the data packet fails to be received.

[00311] In a possible implementation, after the receiving device determines that the data packet fails to be received, the method further includes: the receiving device generates a failure application receipt, where the failure application receipt indicates that the receiving device fails to receive the data packet; and the receiving device sends the failure application receipt to the sending device.

[00312] In a possible implementation, after the receiving device determines that the data packet fails to be received, the method further includes: the receiving device generates an indication application receipt based on a message ID field B, where the indication application receipt indicates that the receiving device fails to receive the data packet, and the message ID field B indicates a latest data packet successfully received by the receiving device; and the receiving device sends the indication application receipt to the sending device.

[00313] In a possible implementation, when the authentication code B is different from the authentication code A, after the receiving device determines that the data packet fails to be received, the method further includes: the receiving device generates information C based on the information B and generates an authentication code C based on the information C; and the receiving device determines, based on the authentication code C, whether the sending device does not receive a latest success application receipt.

[00314] In a possible implementation, when the authentication code C is the same as the authentication code A, that is, the receiving device determines that the sending device does not

receive the latest sent success application receipt, the receiving device sends a success application receipt to the sending device.

[00315] In a possible implementation, when the authentication code C is different from the authentication code A, the receiving device sends a failure application receipt to the sending device.

[00316] In a possible implementation, the data packet further includes a retransmission indication field, and the retransmission indication field indicates that the data packet is a retransmitted data packet or a newly transmitted data packet.

[00317] In a possible implementation, when the authentication code B is different from the authentication code A, after the receiving device determines that the data packet fails to be received, the method further includes: the receiving device determines that the data packet includes a retransmission indication field indicating that the data packet is a newly transmitted data packet, and the receiving device generates and sends, to the sending device, a failure application receipt.

[00318] In a possible implementation, when the authentication code B is different from the authentication code A, after the receiving device determines that the data packet fails to be received, the method further includes: the receiving device determines that the data packet includes a retransmission indication field indicating that the data packet is a retransmitted data packet; the receiving device generates information C based on the information B and generates an authentication code C based on the information C; and the receiving device determines, based on the authentication code C, whether the sending device does not receive a latest success application receipt.

[00319] In a possible implementation, when the authentication code C is the same as the authentication code A, that is, the receiving device determines that the sending device does not receive the latest sent success application receipt, the receiving device sends a success application receipt to the sending device.

[00320] In a possible implementation, when the authentication code C is different from the authentication code A, the receiving device sends a failure application receipt to the sending device.

[00321] In a possible implementation, the receiving device sends, in the second transmission system, a set application receipt to the sending device, where the set application receipt indicates a status of receiving the data packet of the sending device by the receiving device in the first transmission system.

[00322] According to a thirteenth aspect, this application provides a satellite communication system, including a sending device and a receiving device.

[00323] The sending device is configured to generate an authentication code A based on information A and original data, where the information A is sending time information or context information A.

[00324] The sending device is further configured to obtain a data packet based on the authentication code A and the original data.

[00325] The sending device is further configured to send the data packet to the receiving device in a first transmission system.

[00326] The receiving device is configured to receive, in the first transmission system, the data packet sent by the sending device.

[00327] The receiving device is further configured to generate an authentication code B based on the information B and the data packet, where the information B is receiving time information or context information B.

[00328] The receiving device is further configured to determine a receiving status of the data packet based on the authentication code B.

[00329] In a possible implementation, this application provides a communication apparatus, including one or more processors, one or more memories, and a transceiver. The transceiver and the one or more memories are coupled to the one or more processors, the one or more memories are configured to store computer program code, the computer program code includes computer instructions, and when the one or more processors execute the computer instructions, the communication apparatus is enabled to perform the method according to either of the eleventh aspect or the twelfth aspect.

[00330] In a possible implementation, the communication apparatus is a terminal or a satellite network device.

[00331] In a possible implementation, this application provides a computer-readable storage medium. The computer-readable storage medium stores instructions, and when the instructions are run on a computer, the computer is enabled to perform the method according to either of the eleventh aspect or the twelfth aspect.

[00332] In a possible implementation, this application provides a chip or a chip system. The chip or the chip system is applied to a terminal and includes a processing circuit and an interface circuit. The interface circuit is configured to receive code instructions and transmit the code instructions to the processing circuit. The processing circuit is configured to run the code instructions to perform the method according to either of the eleventh aspect or the twelfth aspect.

[00333] According to a fourteenth aspect, this application provides a communication apparatus, including one or more processors, one or more memories, and a transceiver. The transceiver and the one or more memories are coupled to the one or more processors, the one or more memories are configured to store computer program code, the computer program code includes computer instructions, and when the one or more processors execute the computer instructions, the communication apparatus is enabled to perform the method in any one of the first aspect, the fourth

aspect, the seventh aspect, or the ninth aspect or the possible implementations of the first aspect, the fourth aspect, the seventh aspect, or the ninth aspect.

[00334] The communication apparatus may be a terminal or a device in another product form.

[00335] According to a fifteenth aspect, this application provides a communication apparatus, including one or more processors, one or more memories, and a transceiver. The transceiver and the one or more memories are coupled to the one or more processors, the one or more memories are configured to store computer program code, the computer program code includes computer instructions, and when the one or more processors execute the computer instructions, the communication apparatus is enabled to perform the method in any one of the second aspect, the fifth aspect, the eighth aspect, or the tenth aspect or the possible implementations of the second aspect, the fifth aspect, the eighth aspect, or the tenth aspect.

[00336] The communication apparatus may be a satellite network device, or any network element or a combination of a plurality of network elements in the satellite network device.

[00337] According to a sixteenth aspect, this application provides a communication apparatus, including one or more processors, one or more memories, and a transceiver. The transceiver and the one or more memories are coupled to the one or more processors, the one or more memories are configured to store computer program code, the computer program code includes computer instructions, and when the one or more processors execute the computer instructions, the communication apparatus is enabled to perform the method in any one of the third aspect or the sixth aspect or the possible implementations of the third aspect or the sixth aspect.

[00338] The communication apparatus may be any network element or a combination of a plurality of network elements in a satellite network device.

[00339] According to a seventeenth aspect, this application provides a computer storage medium, including computer instructions. When the computer instructions are run on a computer, the computer is enabled to perform the method in any one of the first aspect, the fourth aspect, the seventh aspect, or the ninth aspect or the possible implementations of the first aspect, the fourth aspect, the seventh aspect, or the ninth aspect.

[00340] According to an eighteenth aspect, this application provides a computer storage medium, including computer instructions. When the computer instructions are run on a computer, the computer is enabled to perform the method in any one of the second aspect, the fifth aspect, the eighth aspect, or the tenth aspect or the possible implementations of the second aspect, the fifth aspect, the eighth aspect, or the tenth aspect.

[00341] According to a nineteenth aspect, this application provides a computer storage medium, including computer instructions. When the computer instructions are run on a computer, the computer is enabled to perform the method in any one of the third aspect or the sixth aspect or the

possible implementations of the third aspect or the sixth aspect.

[00342] According to a twentieth aspect, this application provides a computer program product. When the computer program product runs on a computer, the computer is enabled to perform the method in any one of the first aspect, the fourth aspect, the seventh aspect, or the ninth aspect or the possible implementations of the first aspect, the fourth aspect, the seventh aspect, or the ninth aspect.

[00343] According to a twenty-first aspect, this application provides a computer program product. When the computer program product runs on a computer, the computer is enabled to perform the method in any one of the second aspect, the fifth aspect, the eighth aspect, or the tenth aspect or the possible implementations of the second aspect, the fifth aspect, the eighth aspect, or the tenth aspect.

[00344] According to a twenty-second aspect, this application provides a computer program product. When the computer program product runs on a computer, the computer is enabled to perform the method in any one of the third aspect or the sixth aspect or the possible implementations of the third aspect or the sixth aspect.

[00345] According to a twenty-third aspect, this application provides a chip or a chip system. The chip or the chip system is applied to a terminal and includes a processing circuit and an interface circuit. The interface circuit is configured to receive code instructions and transmit the code instructions to the processing circuit. The processing circuit is configured to run the code instructions to perform the method in any one of the first aspect, the fourth aspect, the seventh aspect, or the ninth aspect or the possible implementations of the first aspect, the fourth aspect, the seventh aspect, or the ninth aspect.

BRIEF DESCRIPTION OF DRAWINGS

[00346] FIG. 1A is a schematic diagram of a satellite communication system according to an embodiment of this application;

[00347] FIG. 1B is a schematic diagram of another satellite communication system according to an embodiment of this application;

[00348] FIG. 2A(1) and FIG. 2A(2) are a schematic diagram of a protocol encapsulation architecture of inbound data in a satellite communication system according to an embodiment of this application;

[00349] FIG. 2B(1) and FIG. 2B(2) are a schematic diagram of a protocol parsing architecture of inbound data in a satellite communication system according to an embodiment of this application;

[00350] FIG. 3A(1) to FIG. 3A(3) are a schematic diagram of a protocol encapsulation architecture of outbound data in a satellite communication system according to an embodiment of this application;

[00351] FIG. 3B(1) to FIG. 3B(3) are a schematic diagram of a protocol parsing architecture of outbound data in a satellite communication system according to an embodiment of this application;

[00352] FIG. 4 is a schematic diagram of an authentication verification procedure during inbound transmission in a satellite communication system according to an embodiment of this application;

[00353] FIG. 5 is a flowchart of a method for obtaining a specified key according to an embodiment of this application;

[00354] FIG. 6 is a schematic diagram of a replay attack scenario according to an embodiment of this application;

[00355] FIG. 7A and FIG. 7B are a schematic diagram of a processing procedure of a transmission method according to an embodiment of this application;

[00356] FIG. 8A to FIG. 8C are a schematic diagram of a processing procedure of another transmission method according to an embodiment of this application;

[00357] FIG. 9 is a schematic diagram of an inbound transmission procedure according to an embodiment of this application;

[00358] FIG. 10 is a schematic diagram of an outbound transmission procedure according to an embodiment of this application;

[00359] FIG. 11A and FIG. 11B are a schematic diagram of a processing procedure of another transmission method according to an embodiment of this application;

[00360] FIG. 12 is a schematic diagram of another inbound transmission procedure according to an embodiment of this application;

[00361] FIG. 13 is a schematic diagram of another outbound transmission procedure according to an embodiment of this application;

[00362] FIG. 14 is a schematic diagram of a transmission procedure according to an embodiment of this application;

[00363] FIG. 15A to FIG. 15H are schematic diagrams of a group of interfaces according to an embodiment of this application;

[00364] FIG. 16A is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00365] FIG. 16B is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00366] FIG. 17A is a schematic diagram of another transmission procedure according to an

embodiment of this application;

[00367] FIG. 17B is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00368] FIG. 17C is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00369] FIG. 18A to FIG. 18C are schematic diagrams of another group of interfaces according to an embodiment of this application;

[00370] FIG. 19 is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00371] FIG. 20 is a schematic diagram of an interface according to an embodiment of this application;

[00372] FIG. 21A and FIG. 21B are a schematic diagram of a processing procedure of another transmission method according to an embodiment of this application;

[00373] FIG. 22A and FIG. 22B are a schematic diagram of another inbound transmission procedure according to an embodiment of this application;

[00374] FIG. 23A and FIG. 23B are a schematic diagram of another outbound transmission procedure according to an embodiment of this application;

[00375] FIG. 24A and FIG. 24B are a schematic diagram of another transmission procedure according to an embodiment of this application;

[00376] FIG. 25A to FIG. 25D are schematic diagrams of another group of interfaces according to an embodiment of this application;

[00377] FIG. 26 is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00378] FIG. 27A and FIG. 27B are schematic diagrams of another group of interfaces according to an embodiment of this application;

[00379] FIG. 28A and FIG. 28B are a schematic diagram of another transmission procedure according to an embodiment of this application;

[00380] FIG. 29 is a schematic diagram of an interface according to an embodiment of this application;

[00381] FIG. 30A and FIG. 30B are a schematic diagram of another transmission procedure according to an embodiment of this application;

[00382] FIG. 31A and FIG. 31B are schematic diagrams of another group of interfaces according to an embodiment of this application;

[00383] FIG. 32 is a schematic diagram of another inbound transmission procedure according to an embodiment of this application;

[00384] FIG. 33 is a schematic diagram of another outbound transmission procedure according to an embodiment of this application;

[00385] FIG. 34 is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00386] FIG. 35A and FIG. 35B are a schematic diagram of another transmission procedure according to an embodiment of this application;

[00387] FIG. 36A and FIG. 36B are a schematic diagram of another inbound transmission procedure according to an embodiment of this application;

[00388] FIG. 37A and FIG. 37B are a schematic diagram of another outbound transmission procedure according to an embodiment of this application;

[00389] FIG. 38 is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00390] FIG. 39 is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00391] FIG. 40 is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00392] FIG. 41 is a schematic diagram of another transmission procedure according to an embodiment of this application;

[00393] FIG. 42 is a schematic diagram of a hardware structure according to an embodiment of this application; and

[00394] FIG. 43A and FIG. 43B are schematic diagrams of another group of interfaces according to an embodiment of this application.

DESCRIPTION OF EMBODIMENTS

[00395] The following clearly describes technical solutions in embodiments of this application in detail with reference to the accompanying drawings. In description of embodiments of this application, "/" means "or" unless otherwise specified. For example, A/B may represent A or B. In this specification, "and/or" describes only an association relationship for describing associated objects and indicates that three relationships may exist. For example, A and/or B may indicate the following three cases: Only A exists, both A and B exist, and only B exists.

[00396] The following terms "first" and "second" are merely intended for a purpose of description, and shall not be understood as an indication or implication of relative importance or implicit indication of a quantity of indicated technical features. Therefore, a feature limited by "first" or "second" may explicitly or implicitly include one or more features. In description of

embodiments of this application, "a plurality of" means two or more unless otherwise specified.

[00397] The following describes a satellite communication system 10 according to an embodiment of this application.

[00398] As shown in FIG. 1A, the satellite communication system 10 may include but is not limited to a terminal 100, a satellite 21, a satellite network device 200, a cellular network device 400, a terminal 300, and the like.

[00399] The terminal 100 in a satellite network may send a satellite message to the terminal 300 in a cellular network. Specifically, the terminal 100 may first send a satellite message to the satellite 21. The satellite 21 performs only relay, and may directly forward, to the satellite network device 200 on the ground, the satellite message sent by the terminal 100. The satellite network device 200 may parse, according to a satellite communication protocol, the satellite message forwarded by the satellite 21, and forward, to the cellular network device 400, message content parsed out from the satellite message. The cellular network device 400 may forward the message content to the terminal 300 by using a conventional cellular communication network.

[00400] The terminal 300 in the cellular network may also send a satellite message to the terminal 100 in the satellite network. In an outbound process, the terminal 300 may send an SMS message to a short message service center 25 over a conventional cellular communication network. The short message service center 25 may forward the SMS message of the terminal 300 to the satellite network device 200. The satellite network device 200 may relay the SMS message of the terminal 300 to the terminal 100 by using the satellite 21.

[00401] Optionally, the satellite communication system 10 may further include an emergency rescue platform and an emergency rescue center. The satellite network device 200 may send, to the emergency rescue center by using the emergency rescue platform, a satellite message that is of an emergency rescue type and that is sent by the terminal 100.

[00402] The satellite network device 200 may include but is not limited to a ground transceiver station 22, a central station 23, and a converged communication platform 24. The ground transceiver station 22 may include one or more devices each having a sending function and one or more devices each having a receiving function, or may include one or more devices each having a sending function and a receiving function. This is not limited herein. The ground transceiver station 22 may be configured to perform a data processing function of the satellite network device 200 at a physical (physical, PHY) layer. The central station 23 may be configured to perform a data processing function of the satellite network device 200 at a satellite link control (satellite link control, SLC) layer and a message data convergence protocol (message data convergence protocol, MDCP) layer. The converged communication platform 24 may be configured to perform a data processing function at an application (application, AP) layer. The converged communication

platform 24 may also be referred to as a converged communication gateway 24.

[00403] The cellular network device 400 may include but is not limited to the short message service center (short message service center, SMSC) 25, a home location register (home location register, HLR) 28, a telecommunication business and operation support system (business & operation support system, BOSS) 29, a bootstrapping server (bootstrapping server function, BSF) 41, and a home subscriber server (home subscriber server, HSS) 42. The bootstrapping server 41 and the home subscriber server 42 are not shown in FIG. 1A.

[00404] The short message service center 25 may be configured to forward, to a terminal in the cellular network, data sent by the satellite network device 200, or may be configured to forward data in the cellular network to the satellite network device 200.

[00405] The telecommunication business and operation support system 29 may be configured to perform terminal registration. The telecommunication business and operation support system 29 may allocate a corresponding personal identity (identity, ID) number or the like to a terminal (for example, the terminal 100) during registration. The ID number may be a mobile number of the terminal.

[00406] The bootstrapping server 41 may be configured to receive service requests of the terminal 100 and the satellite network device 200. The bootstrapping server 41 may be further configured to store authentication parameters obtained from the home subscriber server 42. The authentication parameters may include but are not limited to a random (random, RAND), an authentication token (authentication token, AUTN), an expected response (expected response, XRES), a cipher key (cipher key, CK), and an integrity key (integrity key, IK). The bootstrapping server 41 may further generate a session key_network application function (session key_network application function, Ks_NAF) based on the authentication parameters. The bootstrapping server 41 may further send the Ks_NAF to the satellite network device 200. The bootstrapping server 41 may further send some authentication parameters (the RAND and the AUTN) to the terminal 100.

[00407] The home location register 28 and/or the home subscriber server 42 may be configured to generate the authentication parameters and send the authentication parameters to the bootstrapping server 41. The RAND and the AUTN may be used by the terminal 100 to calculate the CK, the IK, and a response (response, RES). The XRES in the authentication parameters may be used by the satellite network device 200 to authenticate whether the terminal 100 is a valid terminal. Only when the satellite network device 200 determines that the XRES is the same as the RES, the satellite network device 200 determines that the terminal 100 is a valid terminal (authentication performed by the satellite network device 200 succeeds), and the satellite network device 200 and the terminal 100 may encrypt/decrypt communication data by using the Ks_NAF. The CK and the IK in the authentication parameters may be used to calculate the Ks_NAF.

[00408] It should be noted that the Ks_NAF is a specified key (also referred to as a first key) in the following embodiments of this application. The specified key may be used to encrypt/decrypt data. Optionally, the specified key may be further used to generate an authentication code.

[00409] It should be noted that a process in which the terminal 100 sends data to the satellite network device 200 is inbound. A process in which the satellite network device 200 sends data to the terminal 100 is outbound.

[00410] In a possible implementation, the ground transceiver station 22 and the central station 23 may be a same device. For example, the device may be a ground central station 31 in a satellite communication system 20 shown in FIG. 1B. The ground central station 31 may be configured to perform a data processing function of a satellite network device 200 at a physical layer, a satellite link control layer, and a message data convergence protocol layer.

[00411] In a possible implementation, a sending device and a receiving device may obtain a specified key in a second transmission system. The sending device may obtain an authentication code A based on the specified key and original data, and send, to the receiving device in a first transmission system, a data packet including the authentication code A. The receiving device may generate an authentication code B based on the specified key and the data packet. The receiving device may determine a receiving status of the data packet based on the authentication code B. In this way, the sending device and the receiving device can update and obtain the specified key by using an abundant supply of air interface resources of a cellular network, thereby saving an air interface resource that is of a satellite network and that is required for negotiating about the specified key. The sending device and the receiving device may alternatively transmit the authentication code and the original data together, to reduce interaction steps required for authentication, thereby further saving an air interface resource of the satellite network.

[00412] It should be noted that the first transmission system may be a satellite transmission system (also referred to as a satellite network or a satellite communication system), for example, the foregoing satellite communication system 10. In some embodiments, the first transmission system may be a BeiDou network transmission system. It should be further noted that the second transmission system is a transmission system that is not the first transmission system. For example, the second transmission system may be a cellular transmission system (also referred to as a cellular network), or the second transmission system may be a wireless local area network (wireless local area network, WLAN) transmission system. This is not limited in embodiments of this application.

[00413] In the following embodiments of this application, a satellite network and a cellular network are used as an example to describe a transmission method.

[00414] The following describes a protocol architecture of inbound data in a satellite communication system 10 according to an embodiment of this application.

[00415] FIG. 2A(1) and FIG. 2A(2) are a schematic diagram of a protocol encapsulation architecture of inbound data in a satellite communication system 10 according to an embodiment of this application.

[00416] As shown in FIG. 2A(1) and FIG. 2A(2), transmission protocol layers in a terminal 100 may be divided into an application layer, a message data convergence protocol layer, a satellite link control layer, and a physical layer.

[00417] When the terminal 100 sends data to a satellite network device 200, a working procedure of transmission protocols in the terminal 100 may be as follows:

[00418] At the AP layer, the terminal 100 generates a first data packet. The first data packet includes original data and a first authentication code generated based on a specified key and the original data. For example, the terminal 100 may generate the first authentication code based on the original data (also referred to as first data) and the specified key, concatenate the first authentication code and the original data together, and perform processing (for example, add a packet header), to obtain the first data packet. The original data may include but is not limited to data entered by a user, a receiving user quantity indication, a receiving user ID, location information of the terminal 100, a voice, an image, an animation, and the like.

[00419] In a possible implementation, the terminal 100 may encrypt, by using the specified key, the first authentication code and the original data that are concatenated together, to obtain encrypted data. The terminal 100 may add packet header information in front of the encrypted data, to obtain the first data packet. The packet header information may include but is not limited to an encryption indication field. The encryption indication field may indicate an encryption algorithm used by the terminal 100 to encrypt data.

[00420] Optionally, before the terminal 100 encrypts the first authentication code and the original data that are concatenated together, the terminal 100 may first compress the first authentication code and the original data that are concatenated together. It may be understood that the packet header information may further include a compression indication field. The compression indication field may indicate a compression algorithm used by the terminal 100 to compress data.

[00421] In a possible implementation, the terminal 100 may encrypt only the original data, to obtain encrypted data. The terminal 100 may add packet header information in front of the encrypted data, to obtain the first data packet. The packet header information may include but is not limited to an encryption indication field. Finally, the terminal 100 adds the first authentication code to the first data packet, to obtain the first data packet including the first authentication code and the encrypted data.

[00422] At the MDCP layer, the terminal 100 may obtain, through an inter-layer interface, the

first data packet delivered by the AP layer, and use the first data packet as an MDCP SDU. At the MDCP layer, the terminal 100 may add padding (padding) data to a trailer of the MDCP SDU to a specified length, and add a redundant length indication field to the MDCP SDU. The redundant length indication field may indicate a length of the padding data. The terminal 100 may split an MDCP SDU to which the padding data and the redundant length indication field are added into one or more pieces of fixed-length MDCP segment data (M_segment), and add a successor indication field to a header of each piece of MDCP segment data, to obtain an MDCP PDU. In other words, the MDCP PDU includes M_segment and the successor indication field. The successor indication field may indicate a sequence of the current MDCP PDU in a plurality of MDCP PDUs in the same MDCP SDU, whether there is an MDCP PDU behind the current MDCP PDU, or whether the current MDCP PDU is a unique MDCP PDU in the MDCP SDU.

[00423] At the SLC layer, the terminal 100 may obtain, through an inter-layer interface, the MDCP PDUs delivered by the MDCP layer, and use the MDCP PDUs as SLC SDUs. At the SLC layer, the terminal 100 may segment the SLC SDU into one or more (for example, four) pieces of fixed-length SLC segment data (S_segment), and add frame header information (also referred to as frame format indication information) to a header of each S_segment, to obtain an SLC PDU. The frame header information may include but is not limited to a user ID field, a total frame quantity field, and a frame sequence number field. The user ID field may indicate a terminal (for example, the terminal 100) that generates the SLC PDU. The total frame quantity field may indicate a total quantity of SLC PDUs included in the SLC SDU to which the SLC PDU belongs. The frame sequence number field may indicate a sequence number of the SLC PDU in the SLC SDU to which the SLC PDU belongs.

[00424] It should be noted that herein, the SLC PDU may be referred to as a second data packet. That is, the terminal 100 may process the first data packet into at least one second data packet by using the MDCP layer and the SLC layer. Alternatively, the MDCP segment may be referred to as a second data packet, and the terminal 100 may process the first data packet into at least one second data packet by using the MDCP layer.

[00425] At the PHY layer, the terminal 100 may obtain, through an inter-layer interface, SLC PDUs delivered by the SLC layer. The terminal 100 may perform a sending processing (for example, encoding, modulation, and spreading) operation on the SLC PDUs, to obtain inbound data. Then, the terminal 100 may send the inbound data to a satellite 21, and the satellite 21 relays the inbound data to the satellite network device 200.

[00426] FIG. 2B(1) and FIG. 2B(2) are a schematic diagram of a protocol parsing architecture of inbound data in a satellite communication system 10 according to an embodiment of this application.

[00427] As shown in FIG. 2B(1) and FIG. 2B(2), transmission protocol layers in a satellite network device 200 may be divided into an application layer, a message data convergence protocol layer, a satellite link control layer, and a physical layer. The satellite network device 200 may include but is not limited to a ground transceiver station 22, a central station 23, and a converged communication platform 24. The ground transceiver station 22 may be configured to be responsible for protocol processing at the PHY layer. The central station 23 may be configured to be responsible for protocol processing at the SLC layer and the MDCP layer. The converged communication platform 24 may be configured to be responsible for protocol processing at the AP layer.

[00428] When the satellite network device 200 receives data sent by a terminal 100, a working procedure of a BeiDou packet transfer protocol in the satellite network device 200 may be as follows:

[00429] At the PHY layer, the satellite network device 200 may obtain inbound data sent by the terminal 100. The satellite network device 200 may deliver data obtained by performing a receiving processing (for example, despreading, demodulation, and decoding) operation on the inbound data to the SLC layer through an inter-layer interface, and use the data as SLC PDUs at the SLC layer.

[00430] At the SLC layer, the satellite network device 200 may concatenate, into one SLC SDU based on frame header information of the SLC PDUs, SLC PDUs belonging to a same SLC SDU of a same terminal. The satellite network device 200 may deliver the SLC SDU to the MDCP layer through an inter-layer interface, and use the SLC SDU as an MDCP PDU at the MDCP layer.

[00431] At the MDCP layer, the satellite network device 200 may concatenate, together in a receiving sequence, all MDCP PDUs belonging to a same MDCP SDU, and remove padding data and a redundant length indication field from the concatenated MDCP PDUs, to obtain an MDCP SDU. The satellite network device 200 may deliver the MDCP SDU to the AP layer through an inter-layer interface, and use the MDCP SDU as a first data packet received at the AP layer. In this case, the SLC layer and the MDCP layer of the satellite network device 200 process the at least one second data packet (the SLC PDUs) to obtain the first data packet, or the MDCP layer of the satellite network device 200 processes at least one second data packet (the MDCP PDUs) to obtain the first data packet.

[00432] At the AP layer, the satellite network device 200 may generate a second authentication code based on a specified key and the first data packet, and determine a receiving status of the first data packet based on the second authentication code. Specifically, the satellite network device 200 may obtain original data in the first data packet, and then generate the second authentication code based on the specified key and the original data. The satellite network device 200 may obtain a

first authentication code in the first data packet, and determine the receiving status of the first data packet by determining, through comparison, whether the first authentication code is the same as the second authentication code. When the first authentication code is the same as the second authentication code, the satellite network device 200 determines that the first data packet is successfully received. That is, the satellite network device 200 determines that the original data in the first data packet is data sent by the terminal 100, and the satellite network device 200 may perform a corresponding operation on the original data (for example, forward the original data to called user equipment in a cellular network). When the first authentication code is different from the second authentication code, the satellite network device 200 determines that the first data packet fails to be received. That is, the satellite network device 200 determines that the original data in the first data packet is not data sent by the terminal 100, and the satellite network device 200 may discard the first data packet.

[00433] In a possible implementation, the first data packet includes encrypted data, and the encrypted data includes an encrypted first authentication code and encrypted original data. The satellite network device 200 may determine, based on a packet header of the first data packet, an encryption algorithm used by the terminal 100. The satellite network device 200 may decrypt the first data packet based on the specified key and the encryption algorithm, to obtain the original data and the first authentication code. The satellite network device 200 may generate the second authentication code based on the specified key and the original data.

[00434] Optionally, after decrypting the encrypted data, the satellite network device 200 may obtain compressed data. After decompressing the compressed data, the satellite network device 200 obtains the first authentication code and the original data.

[00435] In a possible implementation, the first data packet includes encrypted data and the first authentication code. The satellite network device 200 may directly obtain the first authentication code in the first data packet. The satellite network device 200 may perform a decryption operation on the encrypted data based on the specified key and an encryption indication field in packet header information, to obtain the original data.

[00436] In this embodiment of this application, the foregoing protocol processing process is merely an example for description, and a specific protocol processing operation is not limited in this application.

[00437] The following describes a protocol architecture of outbound data in a satellite communication system 10 according to an embodiment of this application.

[00438] FIG. 3A(1) to FIG. 3A(3) are a schematic diagram of a protocol encapsulation architecture of outbound data in a satellite communication system 10 according to an embodiment of this application.

[00439] As shown in FIG. 3A(1) to FIG. 3A(3), transmission protocol layers in a satellite network device 200 may be divided into an application layer, a message data convergence protocol layer, a satellite link control layer, and a physical layer.

[00440] When the satellite network device 200 sends data to a terminal 100, a working procedure of a packet transfer protocol in the satellite network device 200 may be as follows:

[00441] At the AP layer, the satellite network device 200 generates a third data packet. The third data packet includes original data and a fourth authentication code. For example, the satellite network device 200 may generate the fourth authentication code based on the original data (also referred to as third data) and a specified key, concatenate the fourth authentication code and the original data, and perform processing (for example, add a packet header), to obtain the third data packet. The original data may include but is not limited to data, a text, a flag, a voice, an image, an animation, and the like that are sent by a third-party server (for example, a short message service center 25).

[00442] Optionally, the satellite network device 200 may generate the fourth authentication code based on only the original data.

[00443] In a possible implementation, the satellite network device 200 may encrypt, based on the specified key and an encryption algorithm, the original data and the fourth authentication code that are concatenated together, to obtain encrypted data. The satellite network device 200 may add a packet header in front of the encrypted data, to obtain the third data packet. The packet header may include but is not limited to an encryption indication field. The encryption indication field may indicate the encryption algorithm used by the satellite network device 200 to encrypt data.

[00444] Optionally, before encrypting the fourth authentication code and the original data that are concatenated together, the satellite network device 200 may first compress the fourth authentication code and the original data that are concatenated together. It may be understood that the packet header may further include a compression indication field. The compression indication field may indicate a compression algorithm used by the satellite network device 200 to compress data.

[00445] Further, optionally, the satellite network device 200 may compress the fourth authentication code and the original data that are concatenated together, to obtain compressed data. The satellite network device 200 may add the compression indication field in front of the compressed data, and then encrypt, by using the specified key, the compressed data to which the compression indication field is added, to obtain encrypted data.

[00446] In a possible implementation, the satellite network device 200 may encrypt only the original data, to obtain encrypted data. The satellite network device 200 may add packet header information in front of the encrypted data, to obtain the third data packet. The packet header

information may include but is not limited to an encryption indication field. Finally, the satellite network device 200 adds the fourth authentication code to the third data packet, to obtain the third data packet including the fourth authentication code and the encrypted data.

[00447] At the MDCP layer, the satellite network device 200 may obtain, through an inter-layer interface, the third data packet delivered by the AP layer, and use the third data packet as an MDCP SDU. The satellite network device 200 may split the MDCP SDU into one or more pieces of MDCP segment data (M_segment), and add a successor indication field to a header of each piece of MDCP segment data, to obtain an MDCP PDU. In other words, the MDCP PDU includes M_segment and the successor indication field. The successor indication field may indicate a sequence of the current MDCP PDU in the same MDCP SDU, for example, whether the current MDCP PDU is a unique PDU, whether there is an MDCP PDU behind the current MDCP PDU, or whether the current MDCP PDU is the first MDCP PDU.

[00448] For example, a data length of the successor indication field may occupy 2 bits (bit). A meaning of a value of the successor indication field may be as follows:

01: indicating that the MDCP PDU is a start MDCP PDU in a plurality of MDCP PDUs in the MDCP SDU;

10: indicating that the MDCP PDU is an intermediate MDCP PDU in the plurality of MDCP PDUs in the MDCP SDU, namely, another MDCP PDU other than the start MDCP PDU and the last MDCP PDU in the MDCP SDU;

11: indicating that the MDCP PDU is the last MDCP PDU in the plurality of MDCP PDUs in the MDCP SDU; and

00: indicating that the MDCP PDU is a unique MDCP PDU in the MDCP SDU.

[00449] It should be noted that the successor indication field is merely an example, and does not constitute a specific limitation on this embodiment of this application.

[00450] At the SLC layer, the satellite network device 200 may obtain, through an inter-layer interface, the MDCP PDUs delivered by the MDCP layer, and use the MDCP PDUs as SLC SDUs. The satellite network device 200 may segment the SLC SDU into one or more (for example, four) pieces of SLC segment data (S_segment), and add frame header information to a header of each S_segment, to obtain an SLC PDU. The frame header information may include but is not limited to a user ID field, a total frame quantity field, and a frame sequence number field. The user ID field may be used to identify a receiving device (for example, the terminal 100), and a value of the user ID field is an ID number of the receiving device. For detailed descriptions of the total frame quantity field and the frame sequence number field, refer to the foregoing embodiment in FIG. 2A(1) and FIG. 2A(2). Details are not described herein again. It should be noted that herein, the SLC PDU may be referred to as a fourth data packet. The satellite device 200 may process the

third data packet into at least one fourth data packet at the MDCP layer and the SLC layer. Alternatively, the MDCP segment may be referred to as a fourth data packet, and the satellite device 200 may process the third data packet into at least one fourth data packet at the MDCP layer.

[00451] At the PHY layer, the satellite network device 200 may obtain, through an inter-layer interface, SLC PDUs delivered by the SLC layer, and use the SLC PDUs as user frames. The satellite network device 200 may concatenate user frames (also referred to as data frames) of one or more users together, and then add a frame header (for example, a version number) and a check bit, to obtain a physical frame. The satellite network device 200 may perform a sending processing (for example, encoding, modulation, and spreading) operation on the physical frame, to obtain encoded data of a message tributary (an S2C_d tributary). The satellite network device 200 may combine the encoded data of the S2C_d tributary and pilot data (also referred to as a secondary code) of a pilot tributary (an S2C_p tributary) into pilot encoded data, namely, outbound data, and sends the outbound data to a satellite 21. The satellite 21 relays the outbound data to one or more terminals. It may be understood that the pilot data of the S2C_p tributary is related to a satellite beam. When the satellite beam is known information, the pilot data of the S2C_p tributary is also known, and does not need to be decoded. The encoded data of the S2C_d tributary needs to be decoded.

[00452] FIG. 3B(1) to FIG. 3B(3) are a schematic diagram of a protocol parsing architecture of outbound data in a satellite communication system 10 according to an embodiment of this application.

[00453] As shown in FIG. 3B(1) to FIG. 3B(3), transmission protocol layers in a terminal 100 may be divided into an application layer, a message data convergence protocol layer, a satellite link control layer, and a physical layer.

[00454] At the PHY layer, the terminal 100 may capture encoded data of an S2C_d tributary based on a secondary code that is of an S2C_p tributary and that is sent by a satellite network device 200. After capturing the encoded data of the S2C_d tributary, the terminal 100 may perform a receiving processing (for example, despreading, demodulation, and decoding) operation on the encoded data of the S2C_d tributary, to obtain a physical frame. The terminal 100 may extract, from the physical frame, user frames belonging to the terminal 100. The terminal 100 may deliver the user frames to the SLC layer through an inter-layer interface, and use the user frames as SLC PDUs at the SLC layer.

[00455] At the SLC layer, when the user frames received by the terminal 100 are universal data frames, the terminal 100 may concatenate, into one SLC SDU, SLC PDUs belonging to a same SLC SDU. The terminal 100 may deliver the SLC SDU to the MDCP layer through an inter-layer interface, and use the SLC SDU as an MDCP PDU at the MDCP layer. When the user frames

received by the terminal 100 are ACK frames, the terminal 100 may retransmit data/send a next SLC SDU based on a value of a bitmap field.

[00456] At the MDCP layer, the terminal 100 may concatenate, into one MDCP SDU, one or more MDCP PDUs whose packet headers are removed. The terminal 100 may deliver the MDCP SDU to the AP layer through an inter-layer interface, and use the MDCP SDU as a third data packet received at the AP layer. In this case, the SLC layer and the MDCP layer of the terminal 100 process at least one fourth data packet (SLC PDU), to obtain the third data packet.

[00457] At the AP layer, the terminal 100 may generate a third authentication code based on a specified key and the third data packet, and determine a receiving status of the third data packet based on the third authentication code. Specifically, the terminal 100 may obtain original data in the third data packet, and then generate the third authentication code based on the specified key and the original data. The terminal 100 may obtain a fourth authentication code in the third data packet, and determine the receiving status of the third data packet by determining, through comparison, whether the fourth authentication code is the same as the third authentication code. When the fourth authentication code is the same as the third authentication code, the terminal 100 determines that the third data packet is successfully received. That is, the terminal 100 determines that the original data in the third data packet is data sent by the satellite network device 200, and the terminal 100 may perform a corresponding operation on the original data (for example, display the original data on a display screen of the terminal 100 in a form of an SMS message). When the fourth authentication code is different from the third authentication code, the terminal 100 determines that the third data packet fails to be received. That is, the terminal 100 determines that the original data in the third data packet is not data sent by the satellite network device 200, and the terminal 100 may discard the third data packet.

[00458] Optionally, the terminal 100 may generate the third authentication code based on only the original data in the third data packet.

[00459] In a possible implementation, the third data packet includes encrypted data, and the encrypted data includes an encrypted fourth authentication code and encrypted original data. The terminal 100 may determine, based on an encryption indication field of the third data packet, an encryption algorithm used by the satellite network device 200, and then decrypt the encrypted data based on the specified key and the encryption algorithm, to obtain the original data and the fourth authentication code. The terminal 100 may generate the third authentication code based on the specified key and the original data obtained through decryption.

[00460] Optionally, after decrypting the encrypted data, the terminal 100 may obtain compressed data. After decompressing the compressed data, the terminal 100 obtains the fourth authentication code and the original data.

[00461] In a possible implementation, the third data packet includes encrypted data and the fourth authentication code. The terminal 100 may directly extract the fourth authentication code in the third data packet. The terminal 100 may perform a decryption operation on the encrypted data based on the specified key and an encryption indication field in packet header information, to obtain the original data. Then, the terminal 100 obtains the third authentication code based on the original data and the specified key.

[00462] In this embodiment of this application, the foregoing protocol processing process is merely an example for description, and a specific protocol processing operation is not limited in this application.

[00463] The following describes a transmission method in a satellite communication system according to an embodiment of this application.

[00464] FIG. 4 is a schematic diagram of an authentication verification procedure during inbound transmission in a satellite communication system according to an embodiment of this application.

[00465] S401: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about a specified key.

[00466] Specifically, for detailed descriptions of negotiating about the specified key, refer to the embodiment in FIG. 5. Details are not described herein again. After obtaining the specified key by using the cellular network device 400, the terminal 100 and the satellite network device 200 may store the specified key. The terminal 100 and the satellite network device 200 may encrypt/decrypt data by using the specified key.

[00467] In a possible implementation, the specified key obtained by the terminal 100 and the satellite network device 200 in a cellular network can be used within only preset time (for example, 15 days), and available time of the specified key may be referred to as a specified key validity period. After the specified key validity period ends, the terminal 100 and the satellite network device 200 need to return to the cellular network to update the specified key and the specified key validity period.

[00468] S402: The terminal 100 obtains original data.

[00469] The original data may include but is not limited to data (such as text data, image data, audio data, or video data) entered by a calling user (a user of the terminal 100), a called user quantity indication, a called user ID, location information of the terminal 100, and the like.

[00470] In some embodiments, after receiving first input of the calling user, the terminal 100 may obtain the original data in response to the first input, and send the original data to the satellite network device 200. In this embodiment of this application, the input may include but is not limited to a gesture, a voice, and the like. The gesture may include a gesture (for example, tapping) of

directly touching a display screen of the terminal 100 and a floating gesture of not directly touching the display screen.

[00471] S403: The terminal 100 generates a first authentication code based on the specified key and the original data.

[00472] The terminal 100 may generate the first authentication code based on the specified key and the original data by using a specified algorithm. For example, the terminal 100 may obtain the first authentication code for the specified key and the original data by using algorithms approved by the State Password Administration Committee Office.

[00473] S404: The terminal 100 obtains a first data packet based on the first authentication code and the original data.

[00474] The terminal 100 may concatenate the first authentication code and the original data together, to obtain and encrypt, by using the specified key, the first authentication code and the original data that are concatenated together, to obtain encrypted data. The terminal 100 may add packet header information in front of the encrypted data, to obtain the first data packet. The packet header information may include but is not limited to an encryption indication field. The encryption indication field may indicate an encryption algorithm used by the terminal 100. A length of the encryption indication field may be 2 bits. For example, when a value of the encryption indication field is 00, the sending device is indicated not to use an encryption algorithm. When a value of the encryption indication field is 01, the sending device is indicated to use a hash algorithm in the algorithms approved by the State Password Administration Committee Office.

[00475] S405: The terminal 100 may send the first data packet to the satellite network device 200.

[00476] Specifically, for descriptions of a specific procedure in which the terminal 100 sends data to the satellite network device 200, refer to the foregoing embodiment in FIG. 2A(1) and FIG. 2A(2). Details are not described herein again. It should be noted that in a process in which the terminal 100 sends the first data packet to the satellite network device 200, the first data packet includes a user identifier. For example, frame header information added by the terminal 100 at an SLC layer may include a user ID field. The user ID field may be used to identify the terminal 100. A value of the user ID field is an ID number of the terminal 100. The ID number of the terminal 100 may indicate a parameter such as the specified key corresponding to the terminal 100.

[00477] S406: The satellite network device 200 may generate a second authentication code based on the specified key and the first data packet.

[00478] The satellite network device 200 may decrypt the first data packet by using the specified key, to obtain the first authentication code and the original data. The satellite network device 200 may determine, based on the encryption indication field in a packet header, the

encryption algorithm used by the terminal 100. The satellite network device 200 may use the specified key to decrypt the encrypted data in the first data packet by using a decryption algorithm corresponding to the encryption algorithm, to obtain the first authentication code and the original data. For descriptions of a specific procedure in which the satellite network device 200 receives data from the terminal 100, refer to the foregoing embodiment in FIG. 2B(1) and FIG. 2B(2). Details are not described herein again.

[00479] The satellite network device 200 may generate the second authentication code based on the specified key and the original data by using a specified algorithm (for example, a grouping encryption algorithm). The specified algorithm used by the satellite network device 200 to generate the second authentication code is the same as the specified algorithm used by the terminal 100 to generate the authentication code.

[00480] S407: The satellite network device 200 determines whether the first authentication code is the same as the second authentication code.

[00481] The satellite network device 200 may determine a receiving status of the first data packet based on the second authentication code.

[00482] When the satellite network device 200 determines that the first authentication code is different from the second authentication code, the satellite network device 200 determines that the first data packet fails to be received, and may discard the first data packet. Optionally, the satellite network device 200 may perform step S408.

[00483] When the satellite network device 200 determines that the first authentication code is the same as the second authentication code, the satellite network device 200 determines that the first data packet is successfully received. Optionally, the satellite network device 200 may perform step S409.

[00484] S408: The satellite network device 200 sends a failure application receipt to the terminal 100.

[00485] When the satellite network device 200 determines that the first authentication code is different from the second authentication code, the satellite network device 200 may further generate the failure application receipt. The failure application receipt indicates that the satellite network device 200 fails to receive the first data packet. The satellite network device 200 may send the failure application receipt to the terminal 100.

[00486] S409: The satellite network device 200 may send the original data to the cellular network device 400.

[00487] The satellite network device 200 may send the original data to the cellular network device 400 (for example, a short message service center 25). The cellular network device 400 may forward the original data to a called user (for example, a terminal 300) in a specified format (for

example, an SMS message). Optionally, the satellite network device 200 may further perform step S410.

[00488] S410: The satellite network device sends a success application receipt to the terminal 100.

[00489] When the satellite network device 200 determines that the first authentication code is the same as the second authentication code, the satellite network device 200 may further generate the success application receipt. The success application receipt indicates that the satellite network device 200 successfully receives the first data packet. The satellite network device 200 may send the success application receipt to the terminal 100.

[00490] The following describes a flowchart of a method for obtaining a specified key according to an embodiment of this application.

[00491] In a possible implementation, a terminal 100 and a satellite network device 200 may obtain a specified key through negotiation in a cellular network. In this way, the terminal 100 can also perform data encryption and decryption in a satellite network by using the specified key, and does not need to negotiate with the satellite network device about the specified key, thereby ensuring data security while saving an air interface resource of the satellite network device.

[00492] Specifically, the terminal 100 and the satellite network device 200 may obtain the specified key by using a generic bootstrapping architecture (generic bootstrapping architecture, GBA) procedure. For example, as shown in FIG. 5, specific steps in which the terminal 100 and the satellite network device 200 obtain the specified key are as follows:

[00493] S501: The terminal 100 sends a service request 1 to the satellite network device 200.

[00494] When the terminal 100 is in a cellular network, the terminal 100 may send the service request 1 to the satellite network device 200 in the cellular network. The service request 1 may include an identifier of the terminal 100, and the identifier is used to identify an identity of the terminal 100. For example, the service request 1 may be a hypertext transfer protocol get (hypertext transfer protocol GET, HTTP GET) request.

[00495] S502: The satellite network device 200 sends a service response 1 to the terminal 100.

[00496] After receiving the service request 1, after determining, based on the identifier of the terminal 100, that a specified key of the terminal 100 is not stored in the satellite network device 200 or the specified key of the terminal 100 has expired, the satellite network device 200 may send the service response 1 to the terminal 100. The service response 1 may indicate the terminal 100 to obtain a specified key by using a cellular network device 400.

[00497] S503: The terminal 100 sends a service request 2 to a bootstrapping server 41.

[00498] After receiving the service response 1, the terminal 100 may send the service request 2 to the bootstrapping server 41. The service request 2 may include the identifier of the terminal 100.

The service request 2 may indicate the cellular network device 400 to send, to the terminal 100, parameters, such as a random RAND and an authentication token AUTN, required for generating the specified key. For example, the service request 2 may be a hypertext transfer protocol authentication and key agreement (authentication and key agreement, AKA) request.

[00499] S504: The bootstrapping server 41 sends an authentication request to a home subscriber server 42.

[00500] After receiving the service request 2, the bootstrapping server 41 may send the authentication request to the home subscriber server 42. The authentication request includes the identifier of the terminal 100. The authentication request may indicate the home subscriber server 42 to feed back authentication parameters of the terminal 100. For descriptions of the authentication parameters, refer to the foregoing embodiment shown in FIG. 1A. Details are not described herein again. For example, the authentication request may be a multimedia authentication request (multimedia authentication request, MAR).

[00501] S505: The home subscriber server 42 sends the authentication parameters (including the RAND, the AUTN, an XRES, a CK, and an IK) to the bootstrapping server 41.

[00502] After receiving the authentication request, the home subscriber server 42 may obtain the authentication parameters of the terminal 100 based on the identifier of the terminal 100. The home subscriber server 42 pre-stores the identifier of the terminal 100 and the CK and the IK that correspond to the identifier. The home subscriber server 42 may further obtain the random RAND by using a random generator. The home subscriber server 42 may generate the AUTN and the XRES based on the RAND, the IK, and the CK. The home subscriber server 42 may send the generated authentication parameters to the bootstrapping server 41. The identifier of the terminal 100 may include but is not limited to a mobile number, an IP multimedia private identity (IP multimedia private identity, IMPI), a temporary IP multimedia private identity (Temporary IP Multimedia Private Identity, TMPI), and the like of the terminal 100.

[00503] S506: The bootstrapping server 41 sends a service response 2 to the terminal 100.

[00504] After receiving the authentication parameters, the bootstrapping server 41 may send the service response 2 to the terminal 100. The service response 2 may include the RAND and the AUTN.

[00505] S507: The terminal 100 generates the CK, the IK, and an RES based on the RAND and the AUTN.

[00506] After receiving the RAND and the AUTN, the terminal 100 may obtain the CK, the IK, and the RES through calculation based on the RAND and the AUTN by using a SIM card. An algorithm used by the terminal 100 to generate the RES is the same as an algorithm used by the cellular network device 400 to generate the XRES.

[00507] S508: The terminal 100 sends a service request 3 (including the RES) to the bootstrapping server 41.

[00508] After generating the RES, the terminal 100 may send the service request 3 to the cellular network device 400. The service request 3 includes the RES. For example, the service request 3 may be an HTTP GET request whose header field includes the RES.

[00509] S509: The bootstrapping server 41 may determine, through comparison, whether the XRES is the same as the RES.

[00510] After receiving the service request 3 of the terminal 100, the bootstrapping server 41 may verify the identity of the terminal 100 by determining, through comparison, whether the RES is the same as the XRES. If the bootstrapping server 41 determines that the RES is the same as the XRES, the bootstrapping server 41 may perform step S510 and step S511.

[00511] S510: The bootstrapping server 41 may generate a Ks_NAF, a specified key validity period of the Ks_NAF, and a bootstrapping transaction identifier (bootstrapping transaction identifier, B-TID) of the Ks_NAF based on the CK and the IK.

[00512] The bootstrapping server 41 may obtain the Ks_NAF through calculation based on the CK and the IK by using an algorithm for generating the specified key. In addition, the bootstrapping server 41 may generate the B-TID and the specified key validity period that correspond to the Ks_NAF. The Ks_NAF is the specified key of the terminal 100, and may be used to encrypt/decrypt data during data transmission with the satellite network device 200. The B-TID may be used by the satellite network device 200 to obtain the Ks_NAF of the terminal 100 from the bootstrapping server 41. The specified key validity period may indicate validity time of the specified key (Ks_NAF).

[00513] S511: The bootstrapping server 41 may send a service response 3 to the terminal 100.

[00514] The service response 3 may include the specified key validity period and the B-TID. The service response 3 may indicate the terminal 100 to generate the specified key by using the parameters in the service response 2.

[00515] S512: The terminal 100 may generate the Ks_NAF based on the authentication parameters.

[00516] The terminal 100 may obtain the Ks_NAF through calculation based on the CK and the IK by using an algorithm for generating the specified key. The algorithm used by the terminal 100 to generate the specified key is the same as the algorithm used by the cellular network device 400. Within the specified key validity period, in a data transmission process, the terminal 100 may obtain the Ks_NAF (specified key) through calculation by using the authentication parameters, to perform a data encryption/decryption operation.

[00517] S513: The terminal 100 sends a service request 4 (including the B-TID) to the satellite

network device 200.

[00518] After obtaining the Ks_NAF through calculation, the terminal 100 may send the service request 4 to the satellite network device 200. The service request 4 may include the B-TID. The service request 4 may indicate the satellite network device 200 to obtain the specified key of the terminal 100.

[00519] S514: The satellite network device 200 sends a parameter request to the bootstrapping server 41.

[00520] After receiving the service request 4, the satellite network device 200 may send the parameter request to the bootstrapping server 41. The parameter request may include the B-TID. For example, the parameter request may be a bootstrapping-info-request (bootstrapping-info-request, BIR).

[00521] S515: The bootstrapping server 41 sends a parameter response to the satellite network device 200.

[00522] The bootstrapping server 41 may send the parameter response to the satellite network device 200 based on the B-TID of the terminal 100. The parameter response may include the Ks_NAF of the terminal 100 and the specified key validity period. Optionally, the bootstrapping server 41 may generate only the B-TID and the specified key validity period in step S515, and then generate the specified key Ks_NAF after receiving the parameter request of the satellite network device 200.

[00523] S516: The satellite network device 200 sends a service response 4 to the terminal 100.

[00524] The satellite network device 200 may send the service response 4 to the terminal 100 after receiving the specified key returned by the bootstrapping server 41. The service response 4 may indicate that the terminal 100 and the satellite network device 200 can perform a data encryption/decryption operation within the specified key validity period by using the Ks_NAF stored by the terminal 100 and the satellite network device 200. It may be understood that the Ks_NAF is a specified key obtained by the terminal 100 and the satellite network device 200 by using the cellular network device 400.

[00525] In this way, the specified key is updated in the cellular network, and a validity period is preset for the specified key. In a satellite network, the terminal 100 and the satellite network device 200 can perform a data encryption/decryption operation by using the specified key within the validity period. This saves an air interface resource that is of a satellite communication system and that is required for negotiating about the specified key, and also reduces steps of generating the specified key.

[00526] However, because a sending device and a receiving device generate authentication codes based on only original data, when the receiving device repeatedly receives a message of the

sending device, the repeated message may be repeatedly parsed and processed, and the repeated message may be charged for a plurality of times. As shown in FIG. 6, when the sending device is a terminal 100 and the receiving device is a satellite network device 200, if an inbound message of the terminal 100 is intercepted by an attack terminal, and the inbound message is repeatedly sent to the satellite network device 200, a computing resource of the satellite network device 200 may be occupied, and a message fee of the terminal 100 may be repeatedly calculated.

[00527] Therefore, an embodiment of this application provides a transmission method. A sending device may generate an authentication code A based on information A and original data. The sending device may obtain a data packet based on the authentication code A and the original data. The sending device may send the data packet to a receiving device in a first transmission system. After receiving the data packet, the receiving device may generate an authentication code B based on the data packet and information B. The receiving device may determine a receiving status of the data packet based on the authentication code B. The information A and the information B are information updated by the sending device and the receiving device based on transmission, for example, may be time information and updated with time, or may be information about quantities of data packets and respectively updated by the sending device and the receiving device based on a quantity of sent data packets and a quantity of received data packets.

[00528] In this way, because an authentication code A in a repeatedly sent data packet is generated based on information A existing before an update, an authentication code B generated by a receiving device based on updated information B is different from the authentication code A in the repeatedly sent data packet. This indicates that the data packet may be forwarded by an invalid terminal. The receiving device determines that the data packet fails to be received, so that problems of repeated processing and charging do not occur.

[00529] In a possible implementation, information A of a sending device is sending time information, and information B of a receiving device is receiving time information. In this way, when a difference between sending time of the sending device and receiving time of the receiving device exceeds a preset minimum time granularity, the information A is different from the information B, that is, an authentication code A is different from an authentication code B. Therefore, the receiving device cannot parse a data packet sent by the sending device, so that problems of repeated processing and charging do not occur.

[00530] Specifically, a sending device may generate an authentication code A based on information A and original data. The sending device may send, to a receiving device in a first transmission system, a data packet including the authentication code A. The information A is sending time information. After receiving the data packet, the receiving device may generate an authentication code B based on information B and the data packet. The receiving device may

determine a receiving status of the data packet based on the authentication code B. The information B is receiving time information. In this way, when an interval between time at which the sending device generates the authentication code and time at which the receiving device receives the data packet exceeds a minimum time granularity, the receiving device cannot parse the data packet, so that problems of repeated processing and charging do not occur.

[00531] FIG. 7A and FIG. 7B are a schematic diagram of a processing procedure of a transmission method according to an embodiment of this application.

[00532] 1. A sending device generates an authentication code A based on original data and information A.

[00533] The information A is sending time information, and the information A may indicate sending time of a data packet.

[00534] (1) The sending device obtains the sending time of the data packet.

[00535] In an inbound process, the sending time of the data packet may be any time in an entire period from time at which the sending device (a terminal 100) obtains the original data to time, at which the sending device generates the authentication code A, plus offset time (an offset for short). The time at which the terminal 100 obtains the original data may be time at which the terminal 100 receives input of a satellite message sent by a calling user. In this case, the original data includes data entered by the calling user. The time at which the terminal 100 generates the authentication code A may be current time obtained by the terminal 100 by running a program statement for obtaining the sending time of the data packet (for example, by using a get current time function getCurrentTime()). The terminal 100 may determine the sending time of the data packet based on positioning timing of a satellite. Alternatively, the sending time of the first data packet may be represented as time at which the sending device (the terminal 100) delivers the first data packet to an MDCP layer at an AP layer. Alternatively, the sending time of the first data packet may be represented as time that is estimated by the sending device (the terminal 100) and at which the sending device (the terminal 100) sends the first data packet to a receiving device (a satellite network device 200).

[00536] In an outbound process, the sending time of the data packet may be any time in a period from time at which the sending device (the satellite network device 200) obtains the original data to time, at which the sending device generates the authentication code A, plus an offset. The time at which the satellite network device 200 obtains the original data may be time at which the satellite network device 200 receives a service request sent by the terminal 100, or the time at which the satellite network device 200 obtains the original data may be time at which the satellite network device 200 receives a message sent to the terminal 100, time at which the satellite network device 200 sends data to the terminal 100, or the time, at which the satellite network device 200 generates

the authentication code A, plus the offset, and is used to estimate time at which an SLC layer, an MDCP layer, or a physical layer of the satellite network device 200 sends data. The time at which the satellite network device 200 generates the authentication code A may be current time obtained by the satellite network device 200 by running a program statement for obtaining the sending time of the first data packet (for example, by a converged communication platform 24 in the satellite network device 200 by using a get current time function getCurrentTime()). A ground transceiver station 22 or a central station 23 in the satellite network device 200 may determine the sending time of the data packet based on a satellite 21.

[00537] Optionally, in the outbound process, the satellite network device 200 may obtain scheduling time of the data packet based on an outbound data volume and an outbound air interface resource, and the satellite network device 200 may estimate outbound time of the data packet based on the scheduling time of the data packet. That is, the sending time of the data packet of the satellite network device 200 may be the estimated outbound time of the data packet. For example, the converged communication platform 24 in the satellite network device 200 receives schedulable time indicated by the ground transceiver station 22 or the central station 23.

[00538] In some embodiments, the sending time of the data packet may be represented as time at which the sending device delivers the data packet to the MDCP layer at an AP layer.

[00539] (2) The sending device generates the information A based on the sending time of the data packet.

[00540] After obtaining the sending time of the data packet, the sending device may encode the time based on a preset or configured minimum time granularity, to obtain the information A. For example, a time value in front of the preset minimum time granularity in the sending time of the data packet may be extracted, and encoding (for example, binary-decimal encoding or decimal-to-binary conversion) may be performed on the time value, to obtain the information A. For inbound transmission, the sending device, namely, the terminal 100, may encode the time based on a preset minimum time granularity or a minimum time granularity configured for the terminal 100 in a cellular network or a WLAN or in a satellite network, to obtain the information A. For outbound transmission, the sending device, namely, the satellite network device 200, generates the information A. For example, the converged communication platform 24 in the satellite network device 200 performs encoding based on time provided by the ground transceiver station 22 or the central station 23 and a preset or configured minimum time granularity, to generate the information A. For another example, the ground transceiver station or the central station in the satellite network device 200 performs encoding based on the time and a preset or configured minimum time granularity, to obtain the information A, and then notifies the converged communication platform 24 of the information A.

[00541] The preset or configured minimum time granularity may be a minute, half a minute, half an hour, or the like. This is not limited in this application.

[00542] For example, the sending time of the data packet is 2021-08-25 17:23:51. When the minimum time granularity is a minute, a time value that may be obtained by the sending device through extraction based on the preset minimum time granularity is 202108251723.

[00543] For another example, when the minimum time granularity is half a minute, a time value that may be obtained by the sending device through extraction based on the preset minimum time granularity is as follows: For example, the sending device may record, as 0.0 minutes, time that does not exceed 30s, and record, as 0.5 minutes, time that exceeds 30s. In this case, the time value obtained based on the sending time of the data packet is 202108251723.5. For another example, the sending device may record, as 00 seconds, time that does not exceed 30s, and record, as 30 seconds, time that exceeds 30s. In this case, the time value obtained based on the sending time of the data packet is 20210825172330. For another example, the sending device may directly encode a time value in front of a minute to obtain binary data, and then add 1-bit data at the end of the obtained binary data, to indicate the first half minute or the last half minute (for example, 0 represents 1s to 30s, and 1 represents 31s to 60s). For another example, the sending device may divide a value of the sending time of the data packet by a minimum granularity, to obtain an integer value, where the integer value is a time value obtained by the sending device. In this case, the time value obtained by the sending device based on the sending time is 404216503446. It may be understood that actual sending time of the data packet is a product of the time value and a value of the minimum time granularity. In this way, time information may be identified by using an integer quantity of minimum granularities.

[00544] For example, when an encoding manner of the sending device is 8421 encoding in the binary-decimal encoding, the sending device may learn, in the 8421 encoding manner based on a time value 202108251723, that a value of the information A is 0010 0000 0010 0001 0000 1000 0010 0101 0001 0111 0010 0011. When an encoding manner of the sending device is the decimal-to-binary conversion manner, the sending device may learn, through conversion based on a time value 202108251723, that a value of the information A is 101111000011101001011100101110010010 11.

[00545] It should be noted that the foregoing value of the preset minimum time granularity and selection of the encoding manner are merely examples. This is not specifically limited in this application.

[00546] In a possible implementation, the sending device may alternatively obtain a time value of one or more specific time granularities in the sending time of the data packet, and then perform encoding, to obtain the information A. For example, when the sending time of the data packet is

2021-08-25 17:23:51, and the specific time granularities include a month, a minute, and an hour, a time value obtained by the sending device is 082317.

[00547] (3) The sending device obtains the authentication code A based on the information A and the original data.

[00548] The sending device may obtain the authentication code A through calculation based on the information A and the original data by using a specified algorithm (for example, an SM3 hash algorithm).

[00549] Optionally, the sending device may obtain the authentication code A through calculation based on the information A, the original data, and a key by using the specified algorithm.

[00550] 2. The sending device obtains the data packet based on the original data and the authentication code A.

[00551] The sending device may concatenate the authentication code A and the original data together, to obtain the data packet.

[00552] Optionally, the sending device may add packet header information in front of the authentication code A and the original data that are concatenated together, to obtain the data packet. The packet header information may include a service type indication and the like. The service type indication may indicate a service type (for example, a data packet for sending a message to user equipment in a cellular network, or a data packet for requesting data from the satellite network device 200) of the data packet.

[00553] In a possible implementation, the data packet may further include identification information used to identify the data packet, and the identification information may include but is not limited to a message ID field, a count value field, or a sequence number field of the data packet. The identification information may be used by the receiving device to identify the sent data packet. For example, the identification information may be added to an application receipt to indicate a receiving status of the data packet. The sending device may determine, by using the identification information in the application receipt, the receiving status of the data packet corresponding to the identification information.

[00554] 3. The receiving device obtains the authentication code A and the original data based on the data packet.

[00555] After the receiving device receives the data packet sent by the sending device, the receiving device may obtain the authentication code A and the original data from the data packet. For descriptions of sending the data packet by the sending device and receiving the data packet by the receiving device during inbound, refer to the foregoing embodiments shown in FIG. 2A(1) and FIG. 2A(2) and FIG. 2B(1) and FIG. 2B(2). For descriptions of sending the data packet by the

sending device and receiving the data packet by the receiving device during outbound, refer to the foregoing embodiments shown in FIG. 3A(1) to FIG. 3A(3) and FIG. 3B(1) to FIG. 3B(3). Details are not described herein again. It should be noted that the sending device may process the data packet into at least one sub data packet at an MDCP layer and an SLC layer, or the sending device may process the data packet into at least one sub data packet at the MDCP layer. In the inbound process, the data packet may be considered as the foregoing first data packet in FIG. 2A(1) and FIG. 2A(2) or FIG. 2B(1) and FIG. 2B(2), and the sub data packet may be considered as the foregoing second data packet in FIG. 2A(1) and FIG. 2A(2) or FIG. 2B(1) and FIG. 2B(2). In the outbound process, the data packet may be considered as the foregoing third data packet in FIG. 3A(1) to FIG. 3A(3) or FIG. 3B(1) to FIG. 3B(3), and the sub data packet may be considered as the foregoing fourth data packet in FIG. 3A(1) to FIG. 3A(3) or FIG. 3B(1) to FIG. 3B(3).

[00556] 4. The receiving device obtains information B.

[00557] The information B is receiving time information, and the information B may indicate receiving time of the data packet.

[00558] (1) The receiving device obtains the receiving time of the data packet.

[00559] The receiving time of the data packet may be time at which the receiving device obtains the 1st sub data packet of the data packet, time at which the receiving device obtains the first sub data packet of the data packet minus an offset value, or any time in a period from the time at which the receiving device obtains the first sub data packet of the data packet minus the offset value to time at which the receiving device generates the authentication code B. The offset value may be set through configuration or based on a transmission delay (for example, 540 ms) or a processing delay.

[00560] In a specific case, the receiving time may be recorded by using an SLC layer and transferred to an AP layer by using an MDCP layer. The receiving device may record, at the SLC layer, time at which each SLC PDU (sub data packet) is received. When concatenating at least one SLC PDU at the SLC layer based on frame header information to obtain an SLC SDU, the receiving device may record earliest receiving time in receiving time of the at least one SLC PDU as receiving time of the SLC SDU, and upload the SLC SDU and the receiving time corresponding to the SLC SDU to the MDCP layer. After receiving, at the MDCP layer, the SLC SDU and the receiving time corresponding to the SLC SDU that are uploaded from the SLC layer, the receiving device may use the SLC SDU as an MDCP PDU at the MDCP layer. The receiving device may determine, based on a successor indication field, whether the current MDCP PDU is the first MDCP PDU in at least one MDCP PDU. For example, the successor indication field is 00 or 01. When the successor field indicates that data of the MDCP PDU is the first segment of a corresponding MDCP SDU, or the successor indication field indicates that data of the MDCP PDU

is all data of a corresponding MDCP SDU, the receiving device reserves receiving time corresponding to the MDCP PDU, and uses the receiving time as receiving time of the MDCP SDU. The receiving device may upload the MDCP SDU and the receiving time of the MDCP SDU to the AP layer at the MDCP layer. The receiving device may use the MDCP SDU as the data packet at the AP layer. The receiving time corresponding to the MDCP SDU is the time at which the receiving device obtains the 1st sub data packet of the data packet.

[00561] In another specific case, the receiving time may be recorded by using an SLC layer and transferred to an AP layer by using an MDCP layer. An obtaining manner is the same as that in the foregoing case, and details are not described herein again. An offset value is subtracted from time uploaded from the SLC layer. The offset value may be set through configuration or based on a transmission delay (for example, 540 ms).

[00562] In another specific case, the receiving time may be recorded by using an MDCP layer and transferred to an AP layer. The receiving device records, at the MDCP layer, time at which the first MDCP PDU is received. The MDCP layer may perform time recording based on a successor indication. For example, a successor indication field is 00 or 01. When the successor field indicates that data of the MDCP PDU is the first segment of a corresponding MDCP SDU, or the successor indication field indicates that data of the MDCP PDU is all data of a corresponding MDCP SDU, the receiving device reserves the receiving time corresponding to the MDCP PDU, and the receiving device uses the receiving time as receiving time of the MDCP SDU. The receiving device submits the receiving time to the AP layer. The receiving device may use the MDCP SDU as the data packet at the AP layer. The receiving time corresponding to the MDCP SDU is the time at which the receiving device obtains the 1st sub data packet of the data packet.

[00563] In another specific case, the receiving time may be recorded by using an MDCP layer and transferred to an AP layer. An obtaining manner is the same as that in the foregoing case, and details are not described herein again. An offset value is subtracted from time uploaded from the MDCP layer. The offset value may be set through configuration or based on a transmission delay (for example, 540 ms) or a processing delay.

[00564] In another specific case, the receiving time may be time at which an AP layer receives an MDCP SDU or time at which packet assembly of the MDCP SDU submitted from an MDCP layer is completed.

[00565] In another specific case, the receiving time may be time, at which an AP layer receives an MDCP SDU, minus an offset value, or time, at which packet assembly of the MDCP SDU submitted from the MDCP layer is completed, minus an offset value. The offset value may be set through configuration or based on a transmission delay (for example, 540 ms) or a processing delay.

[00566] In another specific case, the receiving time may be current time obtained by running, when the receiving device calculates the authentication code B, a program statement for obtaining the receiving time of the data packet (for example, by using a get current time function getCurrentTime()).

[00567] In another specific case, the receiving time may be current time, obtained by running, when the receiving device calculates the authentication code B, a program statement for obtaining the receiving time of the data packet (for example, by using a get current time function getCurrentTime()), minus an offset value. The offset value may be set through configuration based on a transmission delay (for example, 540 ms) or a processing delay.

[00568] For inbound transmission, the receiving device is the satellite network device 200. The converged communication platform 24 in the satellite network device 200 bears processing of the AP layer, the ground transceiver station 22 or the central station 23 bears processing of the SLC layer and processing of the MDCP layer, and the converged communication platform 24 may request time information from the ground transceiver station 22 or the central station 23.

[00569] For outbound transmission, the receiving device is the terminal device 100.

[00570] (2) The receiving device generates the information B based on the receiving time of the data packet.

[00571] After obtaining the receiving time of the data packet, the receiving device may encode the time based on a preset or configured minimum time granularity, to obtain the information B. For example, a time value in front of the preset minimum time granularity in the receiving time of the data packet may be extracted, and encoding (for example, binary-decimal encoding or decimal-to-binary conversion) may be performed on the time value, to obtain the information B. For outbound transmission, the receiving device, namely, the terminal 100, may encode the time based on a preset minimum time granularity or a minimum time granularity configured for the terminal 100 in a cellular network or in a satellite network, to obtain the information B. For inbound transmission, the receiving device, namely, the satellite network device 200, generates the information B. For example, the converged communication platform 24 in the satellite network device 200 performs encoding based on receiving time information that is of the data packet and that is provided by the ground transceiver station 22 or the central station 23 and a preset or configured minimum time granularity, to generate the information B. For another example, the ground transceiver station or the central station in the satellite network device 200 performs encoding based on the recorded time and a preset or configured minimum time granularity, to obtain the information B, and then transmits the information B to the converged communication platform 24.

[00572] The preset minimum time granularity may be a minute, half a minute, half an hour, or

the like. This is not limited in this application.

[00573] It should be noted that the minimum time granularity and an encoding manner used by the receiving device to generate the information B based on the receiving time of the data packet are the same as those used by the sending device to generate the information A. That is, for descriptions of generating the information B by the receiving device, refer to the foregoing descriptions of generating the information A by the sending device. Details are not described herein.

[00574] In a possible implementation, the receiving device may alternatively extract a time value of one or more specific time granularities in the receiving time of the data packet, and then perform encoding, to obtain the information B.

[00575] In a possible implementation, after obtaining the receiving time of the MDCP SDU at the MDCP layer, the receiving device may use the receiving time of the MDCP SDU as the receiving time of the data packet, generate the information B at the MDCP layer based on the receiving time of the data packet, and upload the MDCP SDU and the information B to the AP layer at the MDCP layer.

[00576] In a possible implementation, after obtaining the receiving time of the SLC SDU at the SLC layer, the receiving device may use the receiving time of the SLC SDU as the receiving time of the data packet, generate the information B at the SLC layer based on the receiving time of the data packet and minimum granularity information and upload the information B to the MDCP layer, and upload the MDCP SDU and the information B to the AP layer at the MDCP layer.

[00577] 5. The receiving device generates the authentication code B based on the information B and the data packet.

[00578] The receiving device may obtain the authentication code B through calculation based on the information B and the original data in the data packet by using a specified algorithm (for example, the SM3 hash algorithm). The specified algorithm of the receiving device is the same as the specified algorithm of the sending device. For example, the sending device may add a specified algorithm indication to a packet header of the data packet, where the specified algorithm indication may indicate the specified algorithm used by the sending device; and the receiving device may determine, based on the specified algorithm indication in the received data packet, the specified algorithm used by the sending device. For another example, the sending device and the receiving device may negotiate about a used specified algorithm in a cellular network.

[00579] 6. The receiving device determines the receiving status of the data packet based on the authentication code B.

[00580] The receiving device may determine the receiving status of the data packet by determining, through comparison, whether the authentication code A is the same as the authentication code B.

[00581] (1) When the authentication code B is the same as the authentication code A, the receiving device determines that the data packet is successfully received. The receiving device may perform a corresponding processing operation on the original data. For example, when the receiving device is the terminal 100, the receiving device may display the original data. When the receiving device is the satellite network device 200, the receiving device may forward the original data to user equipment (for example, a terminal 300) in a cellular network. Optionally, the receiving device may further generate a success application receipt and send the success application receipt to the sending device. The success application receipt may indicate that the receiving device successfully receives the data packet.

[00582] (2) When the authentication code B is different from the authentication code A, the receiving device may obtain information C based on the information B. Specifically, the receiving device may subtract a preset value (for example, 1) from the information B, to obtain the information C. The receiving device may obtain an authentication code C based on the information C and the original data by using a specified authentication algorithm. For example, on a basis that time corresponding to the information B is 2021-09-23 18:00, time corresponding to the information C obtained by subtracting the preset value is 2021-09-23 17:59. The authentication code C is generated based on time information corresponding to the information C. The receiving device may determine, through comparison, whether the authentication code C is the same as the authentication code A.

[00583] (3) When the authentication code A is the same as the authentication code C, the receiving device may determine that the data packet is successfully received. Optionally, the receiving device may further generate and send, to the sending device, a success application receipt. The success application receipt may indicate that the receiving device successfully receives the data packet.

[00584] (4) When the authentication code A is different from the authentication code C, the receiving device may determine that the data packet fails to be received. Optionally, the receiving device may further generate and send, to the sending device, a failure application receipt. The failure application receipt may indicate that the receiving device fails to receive the data packet. In this embodiment, first, the authentication code A may be compared with the authentication code B; and then, when the authentication code A is different from the authentication code B, the information C may be generated, and the authentication code A may be compared with the authentication code C. Alternatively, first, the information B and the information C may be generated, and then the authentication code B and the authentication code C may be generated; and then, the authentication code B and the authentication code C may be compared with the authentication code A. If either of the authentication code B or the authentication code C is the

same as the authentication code A, it indicates that the data packet is successfully received. Optionally, a receiving success application receipt may be fed back. If neither of the authentication code B and the authentication code C is the same as the authentication code A, a sending failure application receipt is fed back.

[00585] In some embodiments, after obtaining the receiving time of the data packet, the receiving device may obtain a receiving time set based on the receiving time of the data packet. The receiving device may obtain the first time value in the receiving time set based on the receiving time of the data packet and the preset minimum time granularity, and then the receiving device subtracts 1 from the first time value to obtain the second time value, and subtract 1 from the second time value to obtain the third time value. By analogy, the receiving device may obtain a receiving time set including n time values. n is a positive integer. The receiving device may perform encoding based on each time value in the receiving time set, to obtain an information B set. The receiving device may perform calculation on each value in the information B set and the original data by using a specified authentication algorithm, to obtain an authentication code set. The receiving device may determine the receiving status of the data packet by comparing a value in the authentication code set with the authentication code A. Provided that one value in the authentication code set is the same as the authentication code A, the receiving device determines that the data packet is successfully received. When no value in the authentication code set is the same as the authentication code A, the receiving device determines that the data packet fails to be received.

[00586] In a possible implementation, before obtaining the data packet, the sending device may encrypt the authentication code A and the original data by using a specified key. The sending device may further add, to the data packet, packet header information including an encryption indication field. After receiving the data packet sent by the sending device, the receiving device may decrypt the data packet based on the encryption indication field and the specified key, to obtain the authentication code A and the original data. In this way, the sending device and the receiving device can ensure data security through data encryption.

[00587] Formats of the sending time of the data packet and the receiving time of the data packet are universal time coordinated (universal time coordinated, UTC), Greenwich mean time (greenwich mean time, GMT), Beijing time, Eastern Pacific time, Western Pacific time, or the like. This is not limited in this embodiment.

[00588] It should be noted that, usually, a difference between the sending time of the data packet of the sending device and the receiving time of the data packet of the receiving device does not exceed the preset minimum time granularity, that is, the receiving device may successfully receive the data packet sent by the sending device.

[00589] In a possible implementation, information A of a sending device is sending time information, and information B of a receiving device is receiving time information. The sending device may generate an authentication code A based on the information A, a specified key, and original data, and then generate a data packet based on the authentication code A and the original data. The receiving device may generate an authentication code B based on the information B, a specified key, and the data packet. In this way, problems of repeated processing and charging do not occur. In addition, because both the sending device and the receiving device generate the authentication codes based on respective stored specified keys, the receiving device may further verify, by using the authentication codes, whether the specified keys of the two parties are the same, to verify validity of the sending device.

[00590] A terminal 100 and a satellite network device 200 may obtain a specified key through negotiation by using a cellular network, as shown in FIG. 5. Alternatively, a terminal 100 and a satellite network device 200 may preset a same specified key.

[00591] In some embodiments, a terminal 100 may obtain a specified key by using an intermediate device. The intermediate device and a satellite network device 200 may first obtain the specified key through negotiation by using a cellular network (for example, for a procedure in which the intermediate device and the satellite network device 200 obtain the specified key through negotiation, refer to the procedure, in which the terminal 100 and the satellite network device 200 obtain the specified key through negotiation, shown in FIG. 5). The intermediate device may establish a communication connection (for example, a Bluetooth connection, a Wi-Fi connection, or a sidelink (sidelink) connection) to the terminal 100. The intermediate device may send the specified key to the terminal 100 through the communication connection.

[00592] Further, to ensure data transmission security, the sending device may concatenate the authentication code A and the original data together, to obtain concatenated data. Then, the sending device uses the specified key to encrypt the concatenated data by using a specified encryption algorithm, to obtain encrypted data. The sending device may add packet header information in front of the encrypted data. The packet header information includes an encryption indication field. The encryption indication field may indicate the specified encryption algorithm (for example, an SM3 hash algorithm) used by the sending device. The receiving device may decrypt the encrypted data in the data packet based on the encryption indication field and the specified key, to obtain the authentication code A and the original data. Then, the receiving device generates the authentication code B based on the original data, the information B, and the specified key. This is shown in FIG. 8A to FIG. 8C. In this way, because the sending device encrypts the data and then sends the encrypted data to the receiving device, data security can be further ensured.

[00593] The following describes an inbound procedure of a transmission method according to

an embodiment of this application.

[00594] A terminal 100 may generate a first authentication code based on first information, a specified key, and first data (also referred to as original data). The first information is sending time information. The terminal 100 may obtain a first data packet based on the first authentication code, the specified key, and the first data. The terminal 100 may send the first data packet to a satellite network device 200. After receiving the first data packet, the satellite network device 200 may generate a second authentication code based on second information, the specified key, and the first data packet. The second information is receiving time information. The satellite network device 200 may determine a receiving status of the first data packet based on the second authentication code. In this way, when the satellite network device 200 receives the repeatedly sent first data packet, because the second information has been updated with time, a generated authentication code is different from the first authentication code in the first data packet. Therefore, the satellite network device 200 determines that the first data packet fails to be received, so that a problem of repeatedly receiving a same data packet does not occur.

[00595] FIG. 9 is a schematic diagram of an inbound transmission procedure according to an embodiment of this application.

[00596] S901: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about a key.

[00597] For descriptions of negotiating about the key by the terminal 100, the satellite network device 200, and the cellular network device 400, refer to the foregoing embodiment shown in FIG. 5. Details are not described herein again. After negotiating about the key, both the terminal 100 and the satellite network device 200 store the specified key.

[00598] S902: The terminal 100 obtains original data.

[00599] After the terminal 100 receives input of a satellite message sent by a user, the terminal 100 may generate, in response to the input, the original data based on content of the satellite message entered by the user. Alternatively, after the terminal 100 receives an indication of a user, for example, when the user wants to initiate a query on a mailbox, or wants to obtain other information from a network, the terminal 100 may generate the original data based on a user request. The original data may include but is not limited to a receiving user quantity indication, a receiving user ID number, data (for example, text data, picture data, or audio data) entered by the user, location information of the terminal 100, and the like.

[00600] S903: The terminal 100 generates a first authentication code based on the specified key, the original data, and first information.

[00601] First, the terminal 100 may obtain sending time of a first data packet. The sending time of the first data packet may be any time in a period from time at which the terminal 100 obtains

the original data to time at which the terminal 100 generates the first authentication code. The time at which the terminal 100 obtains the original data may be time at which the terminal 100 receives input of a satellite message sent by a calling user. In this case, the original data includes data entered by the calling user. The time at which the terminal 100 generates the first authentication code may be current time obtained by the terminal 100 by running a program statement for obtaining the sending time of the first data packet (for example, by using a get current time function getCurrentTime()). The terminal 100 may determine the sending time of the data packet based on positioning timing of a satellite.

[00602] In some embodiments, the sending time of the first data packet may be represented as time at which the terminal 100 delivers the first data packet to an MDCP layer at an AP layer.

[00603] In some other embodiments, the sending time of the first data packet may be represented as time that is estimated by the terminal 100 and at which the terminal 100 sends the first data packet to the satellite network device 200.

[00604] Specifically, for obtaining the sending time of the first data packet by the terminal 100, refer to the foregoing embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00605] Then, the terminal 100 generates the first information based on the sending time of the first data packet. After obtaining the sending time of the first data packet, the terminal 100 may extract a time value in front of a preset minimum time granularity in the sending time of the first data packet, and perform encoding (for example, binary-decimal encoding or decimal-to-binary conversion) on the time value, to obtain the first information. The preset minimum time granularity may be a minute, half a minute, half an hour, or the like. This is not limited in this application. Specifically, for descriptions of generating the first information by the terminal 100, refer to the foregoing embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00606] Finally, the terminal 100 generates the first authentication code based on the specified key, the original data, and the first information. The terminal 100 may obtain the first authentication code through calculation based on the first information, the specified key, and the original data by using a specified algorithm (for example, an SM3 hash algorithm).

[00607] For example, the specified algorithm used by the terminal 100 may be a hash-based message authentication code (hash-based message authentication code, HMAC) algorithm based on the SM3 hash algorithm. A calculation formula of an HMAC is as follows:

$$HMAC=F\{SM3\{(k+\oplus opad)||SM3[(k+\oplus ipad)||(text||context)]\}\}$$

[00608] SM3 is a hash algorithm. k+ may be obtained based on the specified key. A length of k+ may be 64 bytes. 16 most significant bytes are the specified key, and 48 following bytes are all 0. opad is a byte 0x5C repeated 64 times, and ipad is a byte 0x36 repeated 64 times. text is the

original data, and context is the first information. ⊕ is an exclusive OR symbol, and || is a concatenation symbol. A length of output of the SM3 algorithm is 32 bytes. F is a function for extracting data of the first 16 bits from a most significant bit to a least significant bit of input. Output (the HMAC) of F is the first authentication code. A length of the first authentication code is 16 bits.

[00609] S904: The terminal 100 may obtain the first data packet based on the first authentication code and the original data.

[00610] The terminal 100 may concatenate the first authentication code and the original data together, to obtain the first data packet. Optionally, the terminal 100 may further add packet header information in front of the first authentication code and the original data that are concatenated together, to obtain the first data packet. The packet header information may include but is not limited to a service type indication and the like. The service type indication may indicate a service type (for example, a data packet for sending a message to user equipment in a cellular network, or a data packet for requesting data from the satellite network device 200) of the first data packet.

[00611] In a possible implementation, the terminal 100 may further encrypt, by using the specified key, the first authentication code and the original data that are concatenated together, to obtain the first data packet. For specific descriptions, refer to the foregoing embodiment shown in FIG. 8A to FIG. 8C. Details are not described herein again.

[00612] S905: The terminal 100 sends the first data packet to the satellite network device 200.

[00613] In a possible implementation, after sending the first data packet to the receiving device, the terminal 100 may display sending prompt information, for example, display "Sent". The sending prompt information may be used to prompt the user that the terminal 100 has sent the first data packet to the satellite network device 200. The sending prompt information may further include a mark icon. The mark icon may be used to trigger (for example, through tapping) display of an information explanation, for example, "Sent!". Display of an operation suggestion (for example, the message has been sent to the receiving device, and it is not determined whether the message reaches the receiving device) may be triggered through tapping. A form of the sending prompt information is not limited, and may be a text, a picture, an animation, or the like.

[00614] Specifically, the terminal 100 may process the first data packet into at least one second data packet (SLC PDU or MDCP PDU) at the MDCP layer and an SLC layer or the MDCP layer, and then send the at least one second data packet to the satellite network device 200. For specific descriptions of obtaining, by the terminal 100, the at least one second data packet and sending the at least one second data packet to the satellite network device 200, refer to the foregoing embodiments shown in FIG. 2A(1) and FIG. 2A(2) and FIG. 7A and FIG. 7B. Details are not described herein again.

[00615] S906: The satellite network device 200 obtains receiving time of the first data packet, and generates second information based on the receiving time.

[00616] Specifically, the satellite network device 200 may obtain the receiving time of the first data packet in a plurality of manners. For example, when receiving the at least one second data packet at an SLC layer, the satellite network device 200 may record receiving time of each of the at least one second data packet. The satellite network device 200 may concatenate, at the SLC layer based on frame header information of second data packets, second data packets belonging to one SLC SDU, to obtain an SLC SDU. The satellite network device 200 may determine, through comparison, a sequence of receiving time of the second data packets included in the SLC SDU, and use earliest receiving time as receiving time of the SLC SDU. The satellite network device 200 may upload the SLC SDU and the receiving time of the SLC SDU to an MDCP layer at the SLC layer. The satellite network device 200 may use the SLC SDU as an MDCP PDU at the MDCP layer, and obtain an MDCP SDU based on the MDCP PDU. The satellite network device 200 may determine the first MDCP PDU in the MDCP SDU by using successor indication fields of MDCP PDUs, and use, as receiving time of the MDCP SDU, receiving time of an SLC SDU corresponding to the first MDCP PDU. The satellite network device 200 may upload the MDCP SDU and the receiving time of the MDCP SDU to an AP layer at the MDCP layer. The satellite network device 200 may use the MDCP SDU as the first data packet and use the receiving time of the MDCP SDU as the receiving time of the first data packet at the AP layer. For detailed descriptions of obtaining the receiving time of the first data packet by the satellite network device 200, further refer to the foregoing embodiment shown in the inbound process in FIG. 7A and FIG. 7B. Details are not described herein again.

[00617] Specifically, for detailed descriptions of receiving the first data packet by the satellite network device 200, refer to the foregoing embodiments shown in FIG. 2B(1) and FIG. 2B(2) and FIG. 7A and FIG. 7B. Details are not described herein again.

[00618] After obtaining the receiving time (also referred to as fourth information) of the first data packet at the AP layer, the satellite network device 200 may generate the second information based on the fourth information and a preset or configured minimum time granularity. For specific descriptions of generating the second information by the satellite network device 200, refer to the foregoing embodiment, in which the receiving device generates the information B, shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00619] S907: The satellite network device 200 may generate a second authentication code based on the specified key, the original data, and the second information.

[00620] The satellite network device 200 may obtain the second authentication code through calculation based on the second information and the original data in the first data packet by using

a specified algorithm (for example, the SM3 hash algorithm). The specified authentication algorithm of the satellite network device 200 is the same as the specified authentication algorithm of the terminal 100.

[00621] For example, when the specified authentication algorithm used by the terminal 100 may be a hash-based message authentication code (hash-based message authentication code, HMAC) algorithm based on the SM3 hash algorithm, the specified authentication algorithm used by the satellite network device 200 is also the HMAC algorithm based on SM3. An HMAC is calculated as follows:

$$HMAC=F\{SM3\{(k+\oplus opad)||SM3[(k+\oplus ipad)||(text||context)]\}\}$$

[00622] SM3 is a hash algorithm. k+ may be obtained based on the specified key. A length of k+ may be 64 bytes. 16 most significant bytes are the specified key, and 48 following bytes are all 0. opad is a byte 0x5C repeated 64 times, and ipad is a byte 0x36 repeated 64 times. text is the original data, and context is the second information. ⊕ is an exclusive OR symbol, and || is a concatenation symbol. A length of output of the SM3 algorithm is 32 bytes. F is a function for extracting data of the first 16 bits from a most significant bit to a least significant bit of input. Output (the HMAC) of F is the second authentication code. A length of the second authentication code is 16 bits.

[00623] S908: The satellite network device 200 determines whether the first authentication code is the same as the second authentication code.

[00624] The satellite network device 200 may determine a receiving status of the first data packet by determining, through comparison, whether the first authentication code is the same as the second authentication code. When the first authentication code is the same as the second authentication code, the satellite network device 200 may perform step S909, and may further perform step S910. For detailed descriptions of the first authentication code, refer to the authentication code A in the foregoing embodiment shown in FIG. 7A and FIG. 7B. For detailed descriptions of the second authentication code, refer to the authentication code B or the authentication code C in the foregoing embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00625] When the first authentication code is different from the second authentication code, the satellite network device 200 may perform step S911.

[00626] S909: The satellite network device 200 sends the original data to the cellular network device 400.

[00627] The satellite network device 200 determines that the first authentication code is the same as the second authentication code, and determines that the first data packet is successfully received. The satellite network device 200 may perform a corresponding processing operation on

the original data. For example, the satellite network device 200 may forward the original data to user equipment (for example, a terminal 300) in a cellular network.

[00628] Optionally, the satellite network device 200 may further record information about time at which the first data packet is successfully received. For example, the information about the time at which the first data packet is successfully received may be the second information corresponding to the second authentication code. The satellite network device 200 may record the second information, and forward the second information to a network element (for example, a short message service center) in the cellular network. The network element in the cellular network may record sending success time of an inbound message based on the received information about the time at which the first data packet is successfully received, to subsequently send transmission success time information to the terminal 100 in the cellular network, to update a sending status of information for which the terminal 100 fails to receive an application receipt in a satellite network.

[00629] S910: The satellite network device 200 sends an application receipt to the terminal 100, to indicate that the first data packet is successfully sent.

[00630] The satellite network device 200 may further generate a success application receipt (an application receipt indicating that the first data packet is successfully sent). The success application receipt may indicate that the satellite network device 200 successfully receives the data packet. The satellite network device 200 may send the success application receipt to the terminal 100.

[00631] S911: The satellite network device 200 sends an application receipt to the terminal 100, to indicate that the first data packet fails to be sent.

[00632] The satellite network device 200 determines that the first authentication code is different from the second authentication code, and determines that the first data packet fails to be received. The satellite network device 200 may delete the first data packet. The satellite network device 200 may further generate a failure application receipt (an application receipt indicating that the first data packet fails to be sent). The failure application receipt may indicate that the satellite network device 200 fails to receive the data packet. The satellite network device 200 may send the failure application receipt to the terminal 100.

[00633] In a possible implementation, after the satellite network device 200 determines that the first authentication code is different from the second authentication code, the satellite network device 200 may subtract a preset value (for example, 1) from a value of the second information, and then generate a new second authentication code based on adjusted second information, the specified key, and the original data.

[00634] The satellite network device 200 may determine, through comparison, whether the first authentication code is the same as the new second authentication code. When the first authentication code is the same as the new second authentication code, the satellite network device

200 may determine that the data packet is successfully received. The satellite network device 200 may further perform step S909 and step S910.

[00635] When the first authentication code is different from the new second authentication code, the satellite network device 200 may determine that the data packet fails to be received. The satellite network device 200 may further generate and send, to the terminal 100, a failure application receipt. The failure application receipt may indicate that the satellite network device 200 fails to receive the data packet.

[00636] In some embodiments, after receiving the failure application receipt, the terminal 100 may generate and send, to the satellite network device 200, a new first data packet.

[00637] Herein, the success application receipt and the failure application receipt may be collectively referred to as a first application receipt, and the first application receipt may include indication information, indicating, to the user, whether the data packet is successfully received.

[00638] In a possible implementation, after receiving an application receipt (including a failure application receipt or a success application receipt), the terminal 100 may display result prompt information (including success prompt information or failure prompt information) on a display screen. In this way, the user may determine a sending status of the first data packet by using the result prompt information, to avoid repeated sending of a successfully sent satellite message.

[00639] Specifically, the terminal 100 may display success prompt information after receiving a success application receipt (an application receipt indicating that the first data packet is successfully sent). The success prompt information may be used to prompt the user that the first data packet is successfully sent.

[00640] The terminal 100 may display failure prompt information after receiving a failure application receipt (an application receipt indicating that the first data packet fails to be sent). The failure prompt information may be used to prompt the user that the first data packet fails to be sent.

[00641] The following describes an outbound procedure of a transmission method according to an embodiment of this application.

[00642] A satellite network device 200 may generate a fourth authentication code based on sixth information and original data (also referred to as third data). The sixth information is sending time information. The satellite network device 200 may obtain a third data packet based on the fourth authentication code and the original data. The satellite network device 200 may send the third data packet to a terminal 100. After receiving the third data packet, the terminal 100 may generate a third authentication code based on fifth information and the third data packet. The fifth information is receiving time information. The terminal 100 may determine a receiving status of the third data packet based on the third authentication code. In this way, when the terminal 100 receives the repeatedly sent third data packet, because the fifth information has been updated with time, an

authentication code generated based on fifth information is different from the fourth authentication code in the third data packet. Therefore, the terminal 100 determines that the third data packet fails to be received, so that a problem of receiving a repeated data packet does not occur.

[00643] FIG. 10 is a schematic diagram of an outbound transmission procedure according to an embodiment of this application.

[00644] S1001: A satellite network device 200 receives original data sent by a cellular network device 400.

[00645] The satellite network device 200 receives the original data sent by a short message service center 25 in the cellular network device 400. The original data is data sent by a calling user (for example, a user of a terminal 300) in a cellular network to a called user (a user of a terminal 100) in a satellite network (where the data includes but is not limited to text data, picture data, and the like that are entered by the calling user). It should be noted that when forwarding, to the satellite network device 200, the data sent by the terminal 300 to the terminal 100, the cellular network device 400 may also forward an identifier (for example, an ID number or a mobile number of the terminal 100) of the called user to the satellite network device 200.

[00646] In some embodiments, the original data obtained by the satellite network device 200 may be data stored in a memory of the satellite network device 200. For example, the original data may be map data stored in the satellite network device 200.

[00647] In some other embodiments, the original data received by the satellite network device 200 may be data (for example, text data, image data, audio data, or video data) sent by a third-party server to the satellite network device 200.

[00648] S1002: Optionally, the satellite network device 200 receives a service request sent by the terminal 100.

[00649] The service request may be a request for downloading the original data. Herein, a receiving device of the original data is the terminal 100. After receiving the service request of the terminal 100, the satellite network device 200 may perform step S1003 to step 1005.

[00650] S1003: The satellite network device 200 generates a fourth authentication code based on the original data and sixth information.

[00651] First, the satellite network device 200 may obtain sending time of a third data packet. The sending time of the third data packet may be any time in an entire period from time at which the satellite network device 200 obtains the original data to time, at which the satellite network device 200 generates the fourth authentication code, plus an offset. The time at which the satellite network device 200 obtains the original data may be time at which the satellite network device 200 receives the service request sent by the terminal 100, time at which the satellite network device 200 receives the original data sent by the cellular network device 400, time at which the satellite

network device 200 sends data to the terminal 100, or the time, at which the satellite network device 200 generates the fourth authentication code, minus the offset, and is used to estimate time at which an SLC layer, an MDCP layer, or a physical layer of the satellite network device 200 sends data. For example, the time at which the satellite network device 200 generates the fourth authentication code may be current time obtained by the satellite network device 200 by running a program statement for obtaining the sending time of the third data packet (for example, by using a get current time function getCurrentTime()).

[00652] In a possible implementation, the satellite network device 200 may determine the sending time (also referred to as eighth information) of the third data packet at the MDCP layer/the SLC layer (based on a central station 23 or a ground central station 31). Then, the satellite network device 200 generates the sixth information at an AP layer based on the eighth information and a minimum time granularity. Optionally, the satellite network device 200 may determine the sending time of the third data packet at the MDCP layer/the SLC layer, and generate the sixth information based on the sending time of the third data packet and the preset minimum time granularity and then upload the sixth information to the AP layer.

[00653] In some embodiments, the sending time of the third data packet may be represented as time at which the satellite network device 200 delivers the third data packet to the MDCP layer at the AP layer, namely, time at which a converged communication platform 24 delivers the third data packet to the central station 23 or the ground central station 31.

[00654] For obtaining the sending time of the third data packet by the satellite network device 200, refer to the procedure in the embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00655] Then, the satellite network device 200 generates the sixth information based on the sending time of the third data packet. After obtaining the sending time of the third data packet, the satellite network device 200 may encode the time based on a preset or configured minimum time granularity, to obtain the sixth information. For example, the satellite network device 200 may extract a time value in front of the preset or configured minimum time granularity in the sending time of the third data packet, and perform encoding (for example, binary-decimal encoding or decimal-to-binary conversion) on the time value, to obtain the sixth information. The preset or configured minimum time granularity may be a second, a minute, half a minute, half an hour, or the like. This is not limited in this application. Specifically, for descriptions of generating the sixth information by the satellite network device 200, refer to the foregoing embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00656] Finally, the satellite network device 200 generates the fourth authentication code based on the original data and the sixth information. Specifically, the satellite network device 200 may

obtain the fourth authentication code through calculation based on the sixth information and the original data by using a specified algorithm (for example, an SM3 hash algorithm).

[00657] S1004: The satellite network device 200 obtains the third data packet based on the original data and the fourth authentication code.

[00658] The satellite network device 200 may concatenate the fourth authentication code and the original data together, to obtain the third data packet. Optionally, the satellite network device 200 may further add packet header information in front of the fourth authentication code and the original data that are concatenated together, to obtain the third data packet. The packet header information may include but is not limited to a service type indication and the like. The service type indication may indicate a service type (for example, a data packet for sending a satellite message to the terminal 100, or a data packet for sending, to the terminal 100, a quantity of satellite messages sent to the terminal 100) of the third data packet.

[00659] In a possible implementation, the terminal 100 may obtain the fourth authentication code based on a specified key, the sixth information, and the original data.

[00660] In a possible implementation, the terminal 100 may further encrypt, by using the specified key, the fourth authentication code and the original data that are concatenated together, to obtain the third data packet. For specific descriptions, refer to the foregoing embodiment shown in FIG. 8A to FIG. 8C. Details are not described herein again.

[00661] S1005: The satellite network device 200 sends the third data packet to the terminal 100.

[00662] Specifically, the satellite network device 200 may process the third data packet into at least one fourth data packet (SLC PDU) at the MDCP layer and the SLC layer, or the satellite network device 200 may process the third data packet into at least one fourth data packet (MDCP PDU) at the MDCP layer, and then send the at least one fourth data packet to the terminal 100. For specific descriptions of obtaining, by the satellite network device 200, the at least one fourth data packet and sending the at least one fourth data packet to the terminal 100, refer to the foregoing embodiment shown in FIG. 3A(1) to FIG. 3A(3). Details are not described herein again.

[00663] S1006: The terminal 100 obtains receiving time of the third data packet, and generates fifth information based on the receiving time.

[00664] The terminal 100 obtains the receiving time of the third data packet in a plurality of manners. For example, when receiving the at least one fourth data packet at an SLC layer, the terminal 100 may record receiving time of each of the at least one fourth data packet. The terminal 100 may concatenate, at the SLC layer based on frame header information of fourth data packets, fourth data packets belonging to one SLC SDU, to obtain an SLC SDU. The terminal 100 may determine, through comparison, a sequence of receiving time of the fourth data packets included in the SLC SDU, and use earliest receiving time as receiving time of the SLC SDU. The terminal

100 may upload the SLC SDU and the receiving time of the SLC SDU to an MDCP layer at the SLC layer. The terminal 100 may use the SLC SDU as an MDCP PDU at the MDCP layer, and obtain an MDCP SDU based on the MDCP PDU. The terminal 100 may determine the first MDCP PDU in the MDCP SDU by using successor indication fields of MDCP PDUs, and use, as receiving time of the MDCP SDU, receiving time of an SLC SDU corresponding to the first MDCP PDU. The terminal 100 may upload the MDCP SDU and the receiving time of the MDCP SDU to an AP layer at the MDCP layer. The terminal 100 may use the MDCP SDU as the third data packet and use the receiving time of the MDCP SDU as the receiving time of the third data packet at the AP layer. For other detailed descriptions of obtaining the receiving time of the third data packet by the terminal 100, refer to the descriptions of obtaining the receiving time of the data packet by the receiving device in the embodiment in FIG. 7A and FIG. 7B. Details are not described herein again.

[00665] Specifically, for detailed descriptions of receiving the third data packet by theterminal 100, refer to the foregoing embodiments shown in FIG. 3B(1) to FIG. 3B(3) and FIG. 7A and FIG. 7B. Details are not described herein again.

[00666] After obtaining the receiving time of the third data packet, the terminal 100 may generate the fifth information based on the receiving time of the third data packet and a preset or configured minimum time granularity. For specific descriptions of generating the fifth information by the terminal 100, refer to the foregoing embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00667] S1007: The terminal 100 obtains a third authentication code based on the third data packet and the fifth information.

[00668] The terminal 100 may obtain the third authentication code through calculation based on the fifth information and the original data in the third data packet by using a specified authentication algorithm (for example, an SM3 hash algorithm). The specified authentication algorithm of the satellite network device 200 is the same as the specified authentication algorithm of the terminal 100.

[00669] S1008: The terminal 100 determines whether the third authentication code is the same as the fourth authentication code.

[00670] The terminal 100 may determine a receiving status of the third data packet by determining, through comparison, whether the third authentication code is the same as the fourth authentication code. When the third authentication code is the same as the fourth authentication code, the terminal 100 performs step S1009, and optionally, may further perform step S1010.

[00671] Optionally, the terminal 100 may further record information about time at which the third data packet is successfully received, for example, generate the fifth information corresponding to the third authentication code. The information about the time at which the third

data packet is successfully received may be used by the terminal 100 to subsequently send transmission success time information to the satellite device 200 or a network element in a second transmission system when the terminal 100 accesses the second transmission system (for example, a cellular network or a WLAN), to update a sending status of information for which an application receipt fails to be received in a satellite network. This avoids a charging problem.

[00672] When the third authentication code is different from the fourth authentication code, the terminal 100 may perform step S1011.

[00673] S1009: The terminal 100 displays receiving prompt information.

[00674] The terminal 100 determines that the third authentication code is the same as the fourth authentication code, and determines that the third data packet is successfully received. The terminal 100 may perform a corresponding processing operation on the original data. For example, the terminal 100 may display the receiving prompt information. The receiving prompt information may be used to prompt the user that a satellite message sent by user equipment (for example, the terminal 300) in a cellular network is received. The receiving prompt information may include but is not limited to voice prompt information, text prompt information, vibration prompt information, and the like. For example, when the receiving prompt information is text prompt information, the receiving prompt information may be "Received a satellite message from the "terminal 300"". Optionally, the terminal 100 may further the display original data in the third data packet on a display screen.

[00675] S1010: The terminal 100 sends an application receipt to the satellite network device 200, to indicate that the third data packet is successfully received.

[00676] The terminal 100 may further generate a success application receipt (an application receipt indicating that the third data packet is successfully sent). The success application receipt may indicate that the terminal 100 successfully receives the data packet. The terminal 100 may send the success application receipt to the satellite network device 200.

[00677] In some embodiments, after receiving the success application receipt, the satellite network device 200 may delete the original data in the third data packet.

[00678] S1011: The terminal 100 sends an application receipt to the satellite network device 200, to indicate that the third data packet fails to be received.

[00679] The terminal 100 determines that the third authentication code is different from the fourth authentication code, and determines that the third data packet fails to be received. The terminal 100 may delete the third data packet. The terminal 100 may further generate a failure application receipt (an application receipt indicating that the third data packet fails to be sent). The failure application receipt may indicate that the terminal 100 fails to receive the data packet. The terminal 100 may send the failure application receipt to the satellite network device 200.

[00680] In a possible implementation, after the terminal 100 determines that the third authentication code is different from the fourth authentication code, the terminal 100 may subtract a preset value (for example, 1) from a value of the fifth information, and then generate a new third authentication code based on adjusted fifth information and the original data.

[00681] The receiving device may determine, through comparison, whether the fourth authentication code is the same as the new third authentication code. When the fourth authentication code is the same as the new third authentication code, the terminal 100 may determine that the data packet is successfully received. The terminal 100 may further perform step S1010.

[00682] When the fourth authentication code is different from the new third authentication code, the terminal 100 may determine that the data packet fails to be received. The terminal 100 may further generate and send, to the satellite network device 200, a failure application receipt. The failure application receipt may indicate that the terminal 100 fails to receive the data packet.

[00683] In some embodiments, after receiving the failure application receipt, the satellite network device 200 may generate and send, to the terminal 100, a new third data packet.

[00684] Herein, the success application receipt and the failure application receipt may be collectively referred to as a third application receipt, and the third application receipt may include indication information, indicating, to the user, whether the data packet is successfully received.

[00685] This application is not limited to the foregoing embodiments, and further provides the following embodiments. It should be noted that the following embodiments may be used in mutual combination with the foregoing embodiments.

[00686] In a possible implementation, information A of a sending device is context (context) information A, and the context information A may indicate information about a quantity of sent data packets. The information about the quantity of sent data packets is information about a quantity of data packets successfully sent by the sending device. Information B of a receiving device is context information B, and the context information B may indicate information about a quantity of received data packets. The information about the quantity of received data packets is information about a quantity of data packets successfully received by the receiving device (information about a quantity of generated success application receipts). An initial value of the information A is the same as an initial value of the information B. In this way, after successfully parsing, based on the information B, a data packet generated by the sending device based on the information A, the receiving device may update a value of the information B. After the receiving device receives the repeatedly sent data packet, because a value of updated information B is different from a value of the information A existing before an update, that is, an authentication code A is different from an authentication code B, the receiving device cannot parse the data packet

sent by the sending device, so that problems of repeated processing and charging do not occur.

[00687] It should be noted that before the sending device sends the data packet to the receiving device, the sending device and the receiving device may obtain context information. Context information of the sending device may be referred to as the context information A, namely, the information A. Context information of the receiving device may be referred to as the context information B, namely, the information B.

[00688] In a possible implementation, the quantity of data packets successfully sent by the sending device may be a quantity of success application receipts received by the sending device.

[00689] The following describes several manners in which a terminal 100 and a satellite network device 200 obtain context information. Specific descriptions are as follows:

[00690] (1) The terminal 100 and the satellite network device 200 may obtain the context information when obtaining a specified key through negotiation by using a cellular network. For example, the terminal 100, the satellite network device 200, and a cellular network device 400 may perform step S501 to step S515 shown in FIG. 5. After the satellite network device 200 receives a parameter response (including the specified key) sent by a bootstrapping server 41, the satellite network device 200 may set context information of the satellite network device 200. For example, an initial value of the context information of the satellite network device 200 may be X. Then, the satellite network device 200 may send a service response 4 to the terminal 100. The service response 4 may indicate that the terminal 100 and the satellite network device 200 can perform a data encryption/decryption operation within a specified key validity period by using the specified key stored by the terminal 100 and the satellite network device 200. The service response 4 may further include the context information of the satellite network device 200. After receiving the service response 4, the terminal 100 may set an initial value of context information of the terminal 100 to X based on the service response 4. It should be noted that, provided that a value of the context information of the satellite network device 200 is the same as a value of the context information of the terminal 100, even if the initial value of the context information is any value, receiving results of the sending device and the receiving device are not affected.

[00691] (2) The terminal 100 may obtain a specified key and an initial value of context information by using an intermediate device. The intermediate device and the satellite network device 200 may first obtain the specified key, context information of the satellite network device 200, and the context information of the terminal 100 through negotiation in a cellular network by using the foregoing operations. The intermediate device may establish a communication connection (for example, a Bluetooth connection) to the terminal 100. The intermediate device may send the specified key and the context information of the terminal 100 to the terminal 100 through the communication connection.

[00692] (3) Initial values of information A of the terminal 100 and information B of the satellite network device 200 are preset specified values.

[00693] (4) An initial value of information A of the terminal 100 is a data value configured by the satellite network device 200 for the terminal 100.

[00694] FIG. 11A and FIG. 11B are a schematic diagram of a processing procedure of a transmission method according to an embodiment of this application.

[00695] 1. A sending device generates an authentication code A based on original data and information A.

[00696] The information A is context information A, and the information A may indicate information about a quantity of sent data packets. The information about the quantity of sent data packets is information about a quantity of data packets successfully sent by the sending device. Herein, information about a quantity of success application receipts received by the sending device may indicate the information about the quantity of data packets successfully sent by the sending device. That is, after receiving a success application receipt, the sending device may add a preset value to a value of the information A. It should be noted that an increment of the information A is related to the quantity of data packets successfully sent by the sending device.

[00697] The sending device may obtain the authentication code A based on the information A and the original data. For detailed descriptions of obtaining the authentication code A by the sending device, refer to the foregoing embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00698] In a possible implementation, the sending device may generate the authentication code A based on the information A, a specified key, and the original data, and then generate a data packet based on the authentication code A and the original data. A receiving device may generate an authentication code B based on information B, the specified key, and the data packet. In this way, validity of the sending device can be verified by using the specified key, thereby ensuring transmission security.

[00699] 2. The sending device obtains the data packet based on the original data and the authentication code A.

[00700] The sending device may concatenate the authentication code A and the original data together, to obtain the data packet.

[00701] Optionally, the sending device may add packet header information in front of the authentication code A and the original data that are concatenated together, to obtain the data packet. The packet header information may include a service type indication and the like. The service type indication may indicate a service type of the data packet.

[00702] In a possible implementation, the sending device may concatenate the authentication

code A and the original data together, to obtain concatenated data. Then, the sending device uses the specified key to encrypt the concatenated data by using a specified algorithm, to obtain encrypted data. The sending device may add packet header information in front of the encrypted data. The packet header information includes an encryption indication field. The encryption indication field may indicate the specified algorithm (for example, an SM3 hash algorithm) used by the sending device. In this way, because the sending device encrypts the data and then sends the encrypted data to the receiving device, data security can be further ensured.

[00703] The sending device may send the data packet to the receiving device. For descriptions of sending the data packet by the sending device to the receiving device during inbound, refer to the foregoing embodiment shown in FIG. 2A(1) and FIG. 2A(2). For descriptions of sending the data packet by the sending device to the receiving device during outbound, refer to the foregoing embodiment shown in FIG. 3A(1) to FIG. 3A(3). Details are not described herein again.

[00704] In a possible implementation, when the sending device is a terminal 100, after the sending device sends the data packet to the receiving device, the sending device may display sending prompt information. The sending prompt information may be used to prompt a user that the sending device has sent a satellite message to the receiving device.

[00705] 3. The receiving device obtains the authentication code A and the original data based on the data packet.

[00706] After the receiving device receives the data packet sent by the sending device, the receiving device may obtain the authentication code A and the original data from the data packet. For descriptions of receiving the data packet by the receiving device during inbound, refer to the foregoing embodiment shown in FIG. 2B(1) and FIG. 2B(2). For descriptions of receiving the data packet by the receiving device during outbound, refer to the foregoing embodiment shown in FIG. 3B(1) to FIG. 3B(3). Details are not described herein again.

[00707] In a possible implementation, the data packet includes the encryption indication field and the encrypted data. The receiving device may decrypt the encrypted data in the data packet based on the encryption indication field and the specified key, to obtain the authentication code A and the original data.

[00708] 4. The receiving device generates the authentication code B based on the information B and the data packet.

[00709] The receiving device may obtain the authentication code B through calculation based on the information B and the original data in the data packet by using a specified algorithm (for example, the SM3 hash algorithm). The specified algorithm of the receiving device is the same as the specified algorithm of the sending device. For example, the sending device may add a specified algorithm indication to a packet header of the data packet, where the specified algorithm indication

may indicate the specified algorithm used by the sending device; and the receiving device may determine, based on the specified algorithm indication in the received data packet, the specified algorithm used by the sending device. For another example, the sending device and the receiving device may negotiate about a used specified algorithm in a cellular network.

[00710] In a possible implementation, when the sending device generates the authentication code A based on the original data, the information A, and the specified key, the receiving device may generate the authentication code B based on the original data, the information B, and the specified key. The sending device and the receiving device may preset parameters required for generating the authentication codes.

[00711] 5. The receiving device determines a receiving status of the data packet based on the authentication code B.

[00712] The receiving device may determine the receiving status of the data packet by determining, through comparison, whether the authentication code A is the same as the authentication code B.

[00713] (1) When the authentication code B is the same as the authentication code A, the receiving device determines that the data packet is successfully received. The receiving device may perform a corresponding processing operation on the original data. For specific descriptions, refer to the embodiment in FIG. 7A and FIG. 7B.

[00714] The receiving device may update a value of the information B. Specifically, the receiving device may add a preset value to the value of the information B.

[00715] The receiving device may further generate a success application receipt and send the success application receipt to the sending device. The success application receipt may indicate that the receiving device successfully receives the data packet.

[00716] (2) When the authentication code B is different from the authentication code A, the receiving device may determine that the data packet fails to be received. The receiving device may further generate and send, to the sending device, a failure application receipt. The failure application receipt may indicate that the receiving device fails to receive the data packet.

[00717] 6. The sending device determines a sending status of the data packet based on an application receipt.

[00718] The sending device may determine the sending status of the data packet based on the application receipt.

[00719] (1) When the application receipt received by the sending device is a success application receipt indicating that the receiving device successfully receives the data packet, the sending device may determine that the data packet is successfully sent. The sending device may add a preset value to a value of the information A. The preset value added in the sending device is the

same as the preset value added in the receiving device.

[00720] In some embodiments, when the sending device is the terminal 100, after receiving the success application receipt, the sending device may display success prompt information. The success prompt information may be used to prompt the user that the data packet is successfully sent. It should be noted that only after receiving the success application receipt, the sending device can determine that the data packet is successfully sent.

[00721] (2) When the application receipt received by the sending device is a failure application receipt indicating that the receiving device fails to receive the data packet, the sending device may determine that the data packet fails to be sent.

[00722] Optionally, the sending device may retransmit the data packet that fails to be sent.

[00723] In some embodiments, when the sending device is the terminal 100, after receiving the failure application receipt, the sending device may display failure prompt information. The failure prompt information may be used to prompt the user that the data packet fails to be sent.

[00724] The following describes an inbound procedure of a transmission method according to an embodiment of this application.

[00725] A terminal 100 may generate a first authentication code based on first information, a specified key, and first data (also referred to as original data). The first information is first context information, and the first context information indicates information about a quantity of sent data packets. The terminal 100 may obtain a first data packet based on the first authentication code, the specified key, and the original data. The terminal 100 may send the first data packet to a satellite network device 200. After receiving the first data packet, the satellite network device 200 may generate a second authentication code based on second information, the specified key, and the first data packet. The second information is second context information, and the second context information indicates information about a quantity of received data packets. The satellite network device 200 may determine a receiving status of the first data packet based on the second authentication code. In this way, when successfully receiving the first data packet sent by the terminal 100, the satellite network device 200 may update a value of the second information. When the satellite network device 200 repeatedly receives the first data packet, because updated second information is different from the second information existing before the update, an authentication code generated by the satellite network device 200 based on the updated second information is different from the first authentication code in the first data packet. Therefore, the satellite network device 200 determines that the first data packet fails to be received, so that a problem of repeatedly receiving a same data packet does not occur.

[00726] FIG. 12 is a schematic diagram of an inbound transmission procedure according to an embodiment of this application.

[00727] S1201: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about a key, first information, and second information.

[00728] For descriptions of negotiating about the key, the first information, and the second information by the terminal 100, the satellite network device 200, and the cellular network device 400, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again. After negotiating about the key, both the terminal 100 and the satellite network device 200 store the specified key. The terminal 100 stores the first information. The satellite network device 200 stores the second information. An initial value of the first information is the same as an initial value of the second information.

[00729] S1202: The terminal 100 obtains original data.

[00730] S1203: The terminal 100 generates a first authentication code based on the specified key, the original data, and the first information.

[00731] The terminal 100 may obtain the first authentication code through calculation based on the stored first information, the specified key, and the original data by using a specified authentication algorithm (for example, an SM3 hash algorithm).

[00732] S1204: The terminal 100 may obtain a first data packet based on the first authentication code and the original data.

[00733] In a possible implementation, the terminal 100 may further encrypt, by using the specified key, the first authentication code and the original data that are concatenated together, to obtain the first data packet.

[00734] S1205: The terminal 100 sends the first data packet to the satellite network device 200.

[00735] In a possible implementation, after sending the first data packet to the receiving device, the terminal 100 may display sending prompt information, for example, display "Sent". The sending prompt information may be used to prompt a user that the terminal 100 has sent the first data packet to the satellite network device 200. The sending prompt information may further include a mark icon. The mark icon may be used to trigger (for example, through tapping) display of an information explanation, for example, "Sent!". Display of an operation suggestion (for example, the message has been sent to the receiving device, and it is not determined whether the message reaches the receiving device) may be triggered through tapping. A form of the sending prompt information is not limited, and may be a text, a picture, an animation, or the like.

[00736] S1206: The satellite network device 200 may generate a second authentication code based on the specified key, the original data, and the second information.

[00737] S1207: The satellite network device 200 determines whether the first authentication code is the same as the second authentication code.

[00738] The satellite network device 200 may determine a receiving status of the first data

packet by determining, through comparison, whether the first authentication code is the same as the second authentication code. When the first authentication code is the same as the second authentication code, the satellite network device 200 may perform step S1208 to step S1210.

[00739] When the first authentication code is different from the second authentication code, the satellite network device 200 may perform step S1213.

[00740] S1208: The satellite network device 200 updates a value of the second information.

[00741] The satellite network device 200 may add a preset value to the value of the second information. For example, when the value of the second information is 0 and the preset value is 1, an updated value of the second information is 1.

[00742] S1209: The satellite network device 200 sends the original data to the cellular network device 400.

[00743] S1210: The satellite network device 200 sends a success application receipt to the terminal 100.

[00744] S1211: The terminal 100 updates a value of the first information.

[00745] After receiving the success application receipt sent by the satellite network device 200, the terminal 100 may add a preset value to the value of the first information. The preset value added for the first information is the same as the preset value added for the second information, in other words, an updated value of the first information is the same as the updated value of the second information. Optionally, the terminal 100 may further perform step S1212.

[00746] S1212: The terminal 100 displays success prompt information.

[00747] The terminal 100 displays the success prompt information. The success prompt information prompts the user that the first data packet is successfully sent.

[00748] S1213: The satellite network device 200 sends a failure application receipt to the terminal 100.

[00749] Optionally, after receiving the failure application receipt, the terminal 100 may further perform step S1214.

[00750] S1214: The terminal 100 displays failure prompt information.

[00751] The terminal 100 displays the failure prompt information. The failure prompt information prompts the user that the first data packet fails to be sent.

[00752] For specific descriptions of step S1202 to step S1207, step S1209, step S1210, and step S1212, refer to the foregoing embodiment shown in FIG. 9. Details are not described herein again.

[00753] The following describes an outbound procedure of a transmission method according to an embodiment of this application.

[00754] A satellite network device 200 may generate a fourth authentication code based on sixth information and third data (also referred to as original data). The sixth information is sixth context

information, and the sixth context information indicates information about a quantity of sent data packets. The satellite network device 200 may obtain a third data packet based on the fourth authentication code and the original data. The satellite network device 200 may send the third data packet to a terminal 100. After receiving the third data packet, the terminal 100 may generate a third authentication code based on fifth information and the third data packet. The fifth information is fifth context information, and the fifth context information indicates information about a quantity of received data packets. The terminal 100 may determine a receiving status of the third data packet based on the third authentication code. In this way, when successfully receiving the third data packet sent by the satellite network device 200, the terminal 100 may update a value of the fifth information. When the terminal 100 repeatedly receives the third data packet, because updated fifth information is different from the fifth information existing before the update, an authentication code generated by the terminal 100 based on the updated fifth information is different from the fourth authentication code in the third data packet. Therefore, the terminal 100 determines that the third data packet fails to be received, so that a problem of repeatedly receiving a same data packet does not occur.

[00755] FIG. 13 is a schematic diagram of an outbound transmission procedure according to an embodiment of this application.

[00756] S1301: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about fifth information and sixth information.

[00757] The terminal 100 and the satellite network device 200 may obtain respective context information when obtaining a key through negotiation by using the cellular network device 400 in a cellular network. For specific descriptions, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again. Alternatively, the terminal 100 and the satellite network device 200 may establish a communication connection in a cellular network, and obtain respective context information through negotiation. The terminal 100 stores the fifth information. The satellite network device 200 stores the sixth information. An initial value of the fifth information is the same as an initial value of the sixth information.

[00758] S1302: The satellite network device 200 receives original data sent by the cellular network device 400.

[00759] S1303: The satellite network device 200 receives a service request sent by the terminal 100.

[00760] S1304: The satellite network device 200 generates a fourth authentication code based on the original data and the sixth information.

[00761] The satellite network device 200 may generate the fourth authentication code based on the stored sixth information and the original data.

[00762] S1305: The satellite network device 200 obtains a third data packet based on the original data and the fourth authentication code.

[00763] S1306: The satellite network device 200 sends the third data packet to the terminal 100.

[00764] S1307: The terminal 100 obtains a third authentication code based on the third data packet and the fifth information.

[00765] S1308: The terminal 100 determines whether the third authentication code is the same as the fourth authentication code.

[00766] The terminal 100 may determine a receiving status of the third data packet by determining, through comparison, whether the third authentication code is the same as the fourth authentication code. When the third authentication code is the same as the fourth authentication code, the terminal 100 may perform step S1309 to step S1311.

[00767] When the third authentication code is different from the fourth authentication code, the terminal 100 may perform step S1313.

[00768] S1309: The terminal 100 displays receiving prompt information.

[00769] S1310: The terminal 100 updates a value of the fifth information.

[00770] The terminal 100 may add a preset value to the value of the fifth information. For example, when the value of the fifth information is 0 and the preset value is 1, an updated value of the fifth information is 1.

[00771] S1311: The terminal 100 sends a success application receipt to the satellite network device 200.

[00772] S1312: The satellite network device 200 updates a value of the sixth information.

[00773] After receiving the success application receipt sent by the terminal 100, the satellite network device 200 may add a preset value to the value of the sixth information. The preset value added for the sixth information is the same as the preset value added for the fifth information, in other words, an updated value of the sixth information is the same as the updated value of the fifth information.

[00774] S1313: The terminal 100 sends a failure application receipt to the satellite network device 200.

[00775] For specific descriptions of step S1302 to step S1309, step S1311, and step S1313, refer to the foregoing embodiment shown in FIG. 10. Details are not described herein again.

[00776] FIG. 14 is a schematic diagram of a transmission procedure according to an embodiment of this application.

[00777] S1401: After generating an authentication code A based on information A, a sending device obtains a data packet based on the authentication code A and original data, where a value of the information A is X in this case.

[00778] Specifically, for detailed descriptions of generating, by the sending device, the authentication code A and obtaining the data packet, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again.

[00779] S1402: The sending device sends the data packet to a receiving device.

[00780] Specifically, for detailed descriptions of sending the data packet by the sending device to the receiving device, refer to the foregoing embodiments shown in FIG. 2A(1) and FIG. 2A(2) and FIG. 3A(1) to FIG. 3A(3). Details are not described herein again.

[00781] S1403: The receiving device generates an authentication code B based on information B and the data packet, where a value of the information B is X in this case.

[00782] Specifically, for detailed descriptions of generating the authentication code B by the receiving device, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again.

[00783] S1404: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the information B to X+i.

[00784] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet is successfully received. The receiving device may add i to the value of the information B, that is, update the value of the information B to X+i.

[00785] S1405: The receiving device sends a success application receipt to the sending device.

[00786] After determining that the data packet is successfully received, the receiving device may generate the success application receipt, and send the success application receipt to the sending device. The success application receipt may indicate that the receiving device successfully receives the data packet.

[00787] S1406: The sending device updates the value of the information A to X+i.

[00788] After receiving the success application receipt, the sending device may determine that the data packet is successfully sent. The sending device may add i to the value of the information A, that is, update the value of the information A to X+i. The sending device and the receiving device perform updating by using a same value of i.

[00789] S1407: After generating an authentication code A based on the information A, the sending device may obtain a data packet based on the authentication code A and original data, where the value of the information A is X+i in this case.

[00790] S1408: The sending device sends the data packet to the receiving device.

[00791] S1409: The receiving device generates an authentication code B based on the information B and the data packet, where the value of the information B is X+i in this case.

[00792] S1410: The receiving device determines that the authentication code A is the same as

the authentication code B, and updates the value of the information B to X+2i.

[00793] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet is successfully received. The receiving device may add i to the value of the information B, that is, update the value of the information B to X+2i.

[00794] S1411: The receiving device sends a success application receipt to the sending device.

[00795] After determining that the data packet is successfully received, the receiving device may generate the success application receipt, and send the success application receipt to the sending device. The success application receipt may indicate that the receiving device successfully receives the data packet.

[00796] S1412: The sending device updates the value of the information A to X+2i.

[00797] After receiving the success application receipt, the sending device may determine that the data packet is successfully sent. The sending device may add i to the value of the information A, that is, update the value of the information A to X+2i. The sending device and the receiving device perform updating by using the same value of i.

[00798] In this way, the sending device and the receiving device can synchronously update and maintain respective context information, so that the sending device and the receiving device can transmit a data packet, and the receiving device is prevented from repeatedly processing a repeatedly sent data packet.

[00799] The following specifically describes a transmission method according to this application with reference to an application scenario.

[00800] In some inbound application scenarios, after receiving first input of a user, a terminal 100 may send a satellite message (a data packet) to a satellite network device 200 and display sending prompt information. The sending prompt information may be used to prompt the user that the terminal 100 has sent the satellite message to the satellite network device 200. After receiving an application receipt, the terminal 100 may display result prompt information. The result prompt information may be used to prompt the user that the satellite message is successfully sent or fails to be sent. In this way, the user of the terminal 100 can determine a sending status of the satellite message, and resend the satellite message when the satellite message fails to be sent.

[00801] For example, as shown in FIG. 15A, the terminal 100 may display a desktop 1500. The desktop 1500 may include a plurality of application icons (for example, a Clock application icon and a Messaging application icon 1501). The Messaging application icon 1501 may be used to trigger display of a Messaging application interface (for example, a Messaging application interface 1510 shown in FIG. 15B). Optionally, a status bar including icons such as a time identifier icon and a signal identifier icon may be further displayed at the top of the desktop 1500. The signal

identifier icon may be used to prompt the user that the terminal 100 is in a scenario in which no network is available, that is, a scenario in which a communication connection cannot be established to a second transmission system. Optionally, a plurality of tray icons (such as a Phone application icon, a Contacts application icon, and a Camera application icon) may be displayed below the plurality of application icons, and the tray icons remain displayed during page switching. Optionally, the Messaging application icon 1501 may be a tray icon, and is displayed below a plurality of application icons.

[00802] After the terminal 100 detects input (for example, tapping) of the user for the Messaging application icon 1501, the terminal 100 may further display the Messaging application interface 1510 shown in FIG. 15B. As shown in FIG. 15B, the Messaging application interface 1510 may include a message overview display area and a title bar. The message overview display area may be used to display messages sent and received by the terminal 100. The title bar may include but is not limited to a return control, a new message control 1511, and the like. The return control may be used to trigger the terminal 100 to display the desktop 1500. The new message control 1511 may be used to trigger the terminal 100 to create a new satellite message. Optionally, the foregoing status bar may be further displayed at the top of the Messaging application interface 1510.

[00803] After the terminal 100 detects input (for example, tapping) of the user for the new message control 1511, the terminal 100 may further display a contact interface 1520 shown in FIG. 15C. As shown in FIG. 15C, the contact interface 1520 may include at least one contact icon (the contact icon may include but is not limited to a name, a mobile number, and the like of a contact). The at least one contact icon may include a contact icon 1521. The contact icon 1521 may be used to trigger the terminal 100 to determine an ID number of a recipient.

[00804] After the terminal 100 detects input (for example, tapping) of the user for the contact icon 1521, the terminal 100 may display a message detail interface 1530 shown in FIG. 15D. As shown in FIG. 15D, the message detail interface 1530 may include but is not limited to a message editing field 1533, a sending control 1532, and a keyboard area 1531. The message editing field 1533 may be used to display data entered by the user by using the keyboard area 1531. The keyboard area 1531 may be used to receive input of the user to trigger the terminal 100 to display corresponding data. The sending control 1532 may be used to: after receiving input of the user, trigger the terminal 100 to send data in the message editing field 1533 to the recipient. For example, the message editing field 1533 may display text information "X" entered by the user. It should be noted that content displayed in the message editing field 1533 is content entered by the user. Herein, in this embodiment of this application, the content entered by the user is written as "X" merely for better describing the embodiment, and this description does not constitute a limitation on the

content entered by the user.

[00805] It should be noted that, because the terminal 100 is located in a first transmission system, the terminal 100 needs to send the satellite message to a called user (for example, a terminal 300) by using the satellite network device 200. In the descriptions of this embodiment of this application, provided that the satellite network device 200 successfully receives the data packet sent by the terminal 100, the message is successfully sent to the called user by default.

[00806] The terminal 100 receives input of the user for the sending control 1532 shown in FIG. 15D, and in response to the input, the terminal 100 may send, to the satellite network device 200, a data packet including original data (data displayed in the message editing field 1533) entered by the user. Specifically, for detailed descriptions of sending the data packet by the terminal 100 to the satellite network device 200, refer to step S1401 and step S1402 in FIG. 14. For detailed descriptions of receiving and processing the data packet by the satellite network device 200, refer to step S1403 and step S1404 in FIG. 14.

[00807] When the terminal 100 receives the input of the user for the sending control 1532 shown in FIG. 15D, in response to the input, the terminal 100 may further display a message detail interface 1530 shown in FIG. 15E. The message detail interface 1530 may include but is not limited to a message editing field 1533, a message box 1542, and a sending prompt 1543. The message box 1542 may be used to display content of the satellite message that has been sent by the terminal 100 to the satellite network device 200. Herein, the message box 1542 displays "X". The sending prompt 1543 may be used to prompt the user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message box 1542. The sending prompt 1543 may include but is not limited to text prompt information. For example, the sending prompt 1543 may be a character string "Sent". For specific descriptions of the message detail interface 1530, refer to the embodiment shown in FIG. 15D. Details are not described herein again.

[00808] Then, after receiving a success application receipt, the terminal 100 may display success prompt information 1551 shown in FIG. 15F. The success prompt information 1551 may be used to prompt the user that the terminal 100 successfully sends the content in the message box 1542 to the recipient. The success prompt information 1551 may include but is not limited to text prompt information. For example, the success prompt information 1551 may be text prompt information "Sending succeeds". For descriptions of sending the success application receipt by the satellite network device 200 to the terminal 100, refer to step S1405 in FIG. 14. After receiving the success application receipt, the terminal 100 may further update a value of first information to X+i. For specific descriptions of updating the first information by the terminal 100, refer to step S1406 in FIG. 14.

[00809] After updating the value of the first information, the terminal 100 may receive input of

the user for a sending control 1532 shown in FIG. 15F, and in response to the input, the terminal 100 may send, to the satellite network device 200, a data packet including original data (data displayed in a message editing field 1533) entered by the user. The message editing field 1533 may display text information "X+i" entered by the user. Specifically, for detailed descriptions of sending the data packet by the terminal 100 to the satellite network device 200, refer to step S1407 and step S1408 in FIG. 14.

[00810] After the terminal 100 receives the input of the user for the sending control 1532 shown in FIG. 15F, the terminal 100 may further display a message box 1561 and a sending prompt 1562 shown in FIG. 15G. The message box 1561 may be used to display content of a satellite message that has been sent by the terminal 100 to the satellite network device 200. Herein, the message box 1561 displays "X+i". The sending prompt 1562 may be used to prompt the user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message box 1561. For specific descriptions of a message detail interface 1530, refer to the embodiment shown in FIG. 15D. Details are not described herein again.

[00811] After receiving a success application receipt, the terminal 100 may display success prompt information 1571 shown in FIG. 15H. The success prompt information 1571 may be used to prompt the user that the terminal 100 successfully sends the content in the message box 1561 to the recipient.

[00812] The following describes an abnormal case that may occur in embodiments of this application.

[00813] 1. Abnormal case in which a data packet is lost.

[00814] When a sending device sends a data packet to a receiving device, and the receiving device does not receive the data packet of the sending device, transmission of a next data packet between the sending device and the receiving device is not affected. Details are shown in FIG. 16A.

[00815] S1601: After generating an authentication code A based on information A, a sending device obtains a data packet based on the authentication code A and original data, where a value of the information A is X in this case.

[00816] S1602: The sending device fails to send the data packet to a receiving device.

[00817] The data packet is lost during sending, and therefore the receiving device cannot receive the data packet.

[00818] S1603: After generating an authentication code A based on the information A, the sending device may obtain a data packet based on the authentication code A and original data, where the value of the information A is X in this case.

[00819] The receiving device cannot receive the previous data packet sent by the sending device,

and therefore does not update information B of the receiving device. In addition, the receiving device does not send a success application receipt to the sending device, and therefore the value of the information A of the sending device is still X.

[00820] S1604: The sending device sends the data packet to the receiving device.

[00821] S1605: The receiving device generates an authentication code B based on the information B and the data packet, where a value of the information B is X in this case.

[00822] S1606: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the information B to X+i.

[00823] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet is successfully received. The receiving device may add i to the value of the information B, that is, update the value of the information B to X+i.

[00824] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again.

[00825] In this way, when the sending device sends a data packet to the receiving device, the data packet is lost in a sending process, and therefore the receiving device cannot receive the data packet. However, because neither context information of the sending device nor context information of the receiving device is updated, transmission of a subsequent data packet is not affected.

[00826] 2. Abnormal case in which an application receipt is lost.

[00827] When a sending device sends a data packet to a receiving device, the receiving device successfully receives the data packet, and updates a value of information B. A success application receipt sent by the receiving device to the sending device is lost in a sending process, and therefore the sending device cannot receive the success application receipt, and does not update a value of information A. In this way, context information of the sending device is inconsistent with context information of the receiving device, affecting transmission of a subsequent data packet. Details are shown in FIG. 16B.

[00828] S1611: After generating an authentication code A based on information A, a sending device obtains a data packet based on the authentication code A and original data, where a value of the information A is X in this case.

[00829] S1612: The sending device sends the data packet to a receiving device.

[00830] S1613: The receiving device generates an authentication code B based on information B and the data packet, where a value of the information B is X in this case.

[00831] S1614: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the information B to X+i.

[00832] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet is successfully received. The receiving device may add i to the value of the information B, that is, update the value of the information B to X+i.

[00833] S1615: The receiving device fails to send a success application receipt to the sending device.

[00834] The success application receipt is lost during sending, and therefore the sending device cannot receive the success application receipt.

[00835] S1616: After generating an authentication code A based on the information A, the sending device obtains a data packet based on the authentication code A and original data, where the value of the information A is X in this case.

[00836] The sending device cannot receive the success application receipt sent by the receiving device, and therefore cannot determine a sending status of the previous data packet, and cannot update the information A. Therefore, the value of the information A is still X.

[00837] S1617: The sending device sends the data packet to the receiving device.

[00838] S1618: The receiving device generates an authentication code B based on the information B and the data packet, where the value of the information B is X+i in this case.

[00839] S1619: The receiving device determines that the authentication code A is different from the authentication code B.

[00840] The receiving device determines that the authentication code A is different from the authentication code B, and determines that the data packet fails to be received.

[00841] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again.

[00842] In this way, when the sending device sends a data packet to the receiving device, the receiving device successfully receives the data packet, and therefore updates the value of the information B, and sends a success application receipt to the sending device. However, the sending device fails to receive the success application receipt, and therefore the information A of the sending device is not updated. Therefore, the information A is different from the information B, affecting transmission of a subsequent data packet.

[00843] Therefore, to ensure that a sending device and a receiving device can further transmit a subsequent data packet after information A is inconsistent with information B, the sending device and the receiving device may reset values of respective context information. In this way, the sending device and the receiving device can continue to transmit a data packet.

[00844] In a possible implementation, when determining that a data packet fails to be received, a receiving device may reset information B to a preset initial value. After receiving a failure

application receipt, the sending device may also reset information A to the preset initial value. In this way, when the information A is not synchronized with the information B, values of the information A and the information B may be adjusted to a same value, so that the sending device and the receiving device can continue to transmit a data packet. For example, this is shown in FIG. 17A.

[00845] S1701: After generating an authentication code A based on information A, a sending device obtains a data packet based on the authentication code A and original data, where a value of the information A is X in this case.

[00846] S1702: The sending device sends the data packet to a receiving device.

[00847] S1703: The receiving device generates an authentication code B based on information B and the data packet, where a value of the information B is Y in this case.

[00848] X is different from Y.

[00849] S1704: The receiving device determines that the authentication code A is different from the authentication code B, and updates the value of the information B to Z.

[00850] The receiving device may determine a receiving status of the data packet by determining, through comparison, whether the authentication code A is the same as the authentication code B. The receiving device determines that the authentication code A is different from the authentication code B, and determines that the data packet fails to be received.

[00851] The receiving device may adjust the value of the information B to the preset initial value Z.

[00852] S1705: The receiving device sends a failure application receipt to the sending device.

[00853] After determining that the data packet fails to be received, the receiving device may generate an application receipt (the failure application receipt) indicating that the data packet fails to be received. The receiving device may send the failure application receipt to the sending device.

[00854] S1706: The sending device updates the value of the information A to Z.

[00855] After receiving the failure application receipt, the sending device determines that the data packet fails to be sent, and updates the value of the information A to Z. Context information of the sending device and context information of the receiving device are adjusted to a same value.

[00856] However, when the sending device does not receive the failure application receipt sent by the receiving device, the value of the information A is still different from the value of the information B. Therefore, in a possible implementation, when determining that a data packet fails to be received, a receiving device may merely send a failure application receipt to a sending device, and does not change a value of information B. After receiving the failure application receipt, the sending device may reset information A to a preset initial value. The sending device may further send the preset initial value to the receiving device, and the receiving device may adjust the value

of the information B to the preset initial value after receiving the preset initial value. For example, this is shown in FIG. 17B.

[00857] S1711: After generating an authentication code A based on information A, a sending device obtains a data packet based on the authentication code A and original data, where a value of the information A is X in this case.

[00858] S1712: The sending device sends the data packet to a receiving device.

[00859] S1713: The receiving device generates an authentication code B based on information B and the data packet, where a value of the information B is Y in this case.

[00860] X is different from Y.

[00861] S1714: The receiving device determines that the authentication code A is different from the authentication code B.

[00862] The receiving device may determine a receiving status of the data packet by determining, through comparison, whether the authentication code A is the same as the authentication code B. The receiving device determines that the authentication code A is different from the authentication code B, and determines that the data packet fails to be received.

[00863] S1715: The receiving device sends a failure application receipt to the sending device.

[00864] After determining that the data packet fails to be received, the receiving device may generate an application receipt (the failure application receipt) indicating that the data packet fails to be received. The receiving device may send the failure application receipt to the sending device.

[00865] S1716: The sending device updates the value of the information A to Z.

[00866] After receiving the failure application receipt, the sending device determines that the data packet fails to be sent, and updates the value of the information A to Z.

[00867] S1717: The sending device sends the value of the information A to the receiving device.

[00868] For example, the sending device may encapsulate the value of the information A as a data packet, and then send, to the receiving device, the data packet including the value of the information A.

[00869] That is, in an inbound process, after adjusting a value of first information to a preset value, a terminal 100 may send third information to a satellite network device 200. A value of the third information is the same as an adjusted value of the first information.

[00870] In an outbound process, after adjusting a value of sixth information to a preset value, the satellite network device 200 may send seventh information to the terminal 100. A value of the seventh information is the same as an adjusted value of the sixth information.

[00871] Optionally, the preset value is an initial value.

[00872] S1718: The receiving device updates the value of the information B to Z.

[00873] After receiving the value of the information A, the receiving device may adjust the

value of the information B to be the same as the value of the information A, that is, adjust the value of the information B to the preset initial value Z.

[00874] However, when an attack terminal intercepts the preset initial value and repeatedly sends the preset initial value to the receiving device, the receiving device keeps resetting the value of the information B of the receiving device, and consequently the sending device and the receiving device cannot normally communicate with each other. In addition, because the reason why the information A is inconsistent with the information B is mostly that the sending device does not receive a success application receipt sent by the receiving device, the value of the information B is greater than the value of the information A by the preset value.

[00875] Therefore, in a possible implementation, after failing to receive a data packet, a receiving device does not adjust a value of information B, and a sending device may add a preset value to a value of information A after receiving a failure application receipt. In this way, after receiving the application receipt, the sending device may adjust the value of the information A, so that the information A is the same as the information B.

[00876] It should be noted that, herein, a quantity of data packets successfully sent by the sending device may be a sum of a quantity of success application receipts received by the sending device and a quantity of unreceived success application receipts determined by the sending device based on failure application receipts.

[00877] The following describes the foregoing possible implementation with reference to a scenario. Details are shown in FIG. 17C.

[00878] S1721: After generating an authentication code A based on information A, a sending device obtains a data packet based on the authentication code A and original data, where a value of the information A is X in this case.

[00879] S1722: The sending device sends the data packet to a receiving device.

[00880] In an inbound process, the sending device is a terminal 100, and the receiving device is a satellite network device 200. After sending the data packet to the satellite network device 200, the terminal 100 may display a message detail interface 1800 shown in FIG. 18A. The message detail interface 1800 may include a message box 1801 and a sending prompt 1802. The message box 1801 may be used to display content of a satellite message that has been sent by the terminal 100 to the satellite network device 200. Herein, the message box 1801 displays message content, for example, "X". The sending prompt 1802 may be used to prompt a user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message box 1801. For specific descriptions of the message detail interface 1800, refer to the embodiment shown in FIG. 15D. Details are not described herein again. It should be noted that any content displayed in the message box described in this embodiment of this application is content entered by the user in a

satellite message. Herein, in this embodiment of this application, the content is written as "X" merely for better describing the embodiment, and this description does not constitute a limitation on the content entered by the user.

[00881] S1723: The receiving device generates an authentication code B based on information B and the data packet, where a value of the information B is X in this case.

[00882] S1724: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the information B to X+i.

[00883] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet is successfully received. The receiving device may add i to the value of the information B, that is, update the value of the information B to X+i.

[00884] S1725: The receiving device fails to send a success application receipt to the sending device.

[00885] The success application receipt is lost during sending, and therefore the sending device cannot receive the success application receipt.

[00886] S1726: After generating an authentication code A based on the information A, the sending device obtains a data packet based on the authentication code A and original data, where the value of the information A is X in this case.

[00887] The sending device cannot receive the success application receipt sent by the receiving device, and therefore cannot determine a sending status of the previous data packet, and cannot update the information A. Therefore, the value of the information A is still X.

[00888] S1727: The sending device sends the data packet to the receiving device.

[00889] In the inbound process, the sending device is the terminal 100, and the receiving device is the satellite network device 200. After sending the data packet to the satellite network device 200, the terminal 100 may display a message box 1811 and a sending prompt 1812 shown in FIG. 18B. The message box 1811 may be used to display content of a satellite message that has been sent by the terminal 100 to the satellite network device 200. Herein, the message box 1811 displays "X". The sending prompt 1812 may be used to prompt the user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message box 1811. For specific descriptions of a message detail interface 1800, refer to the embodiment shown in FIG. 15D. Details are not described herein again.

[00890] S1728: The receiving device generates an authentication code B based on the information B and the data packet, where the value of the information B is X+i in this case.

[00891] S1729: The receiving device determines that the authentication code A is different from the authentication code B.

[00892] The receiving device determines that the authentication code A is different from the authentication code B, and determines that the data packet fails to be received.

[00893] S1730: The receiving device sends a failure application receipt to the sending device.

[00894] S1731: The sending device updates the value of the information A to X+i.

[00895] After receiving the failure application receipt, the sending device may determine that the current data packet fails to be received. In addition, because the sending device sends only two data packets, the sending device may determine that the value of the information B is updated, that is, the sending device may determine that the receiving device successfully receives the previous data packet of the sending device. The sending device may determine that the previous data packet is successfully sent and the current data packet fails to be sent, and the sending device may add a preset value to the value of the information A, that is, adjust the value of the information A to X+i.

[00896] In the inbound process, the sending device is the terminal 100, and the receiving device is the satellite network device 200. After receiving the failure application receipt, the terminal 100 may display success prompt information 1821 and failure prompt information 1822 shown in FIG. 18C. The success prompt information 1821 may be used to prompt the user that the terminal 100 successfully sends the content in the message box 1801 to a recipient. The failure prompt information 1822 may be used to prompt the user that the terminal 100 fails to send the content in the message box 1811 to the recipient. The failure prompt information 1822 may include but is not limited to text prompt information. For example, the failure prompt information 1822 may include text prompt information "Sending fails".

[00897] It should be noted that only after receiving an application receipt, the terminal 100 displays result prompt information.

[00898] In this way, even if the failure application receipt is intercepted by an attack terminal, the sending device does not repeatedly update the value of the information A.

[00899] In some embodiments, when a data packet sent by a sending device is lost in a sending process, and a receiving device does not receive the data packet of the sending device, transmission of a next data packet between the sending device and the receiving device is not affected. The sending device may further determine, based on a success application receipt of the next sent data packet, that the previous data packet fails to be received.

[00900] The following describes the foregoing possible implementation with reference to a scenario. Details are shown in FIG. 19.

[00901] S1901: After generating an authentication code A based on information A, a sending device obtains a data packet based on the authentication code A and original data, where a value of the information A is X in this case.

[00902] S1902: The sending device fails to send the data packet to a receiving device.

[00903] The data packet is lost during sending, and therefore the receiving device cannot receive the data packet.

[00904] In an inbound process, the sending device is a terminal 100, and the receiving device is a satellite network device 200. After sending the data packet to the satellite network device 200, the terminal 100 may display a message detail interface 1800 shown in FIG. 18A. For detailed descriptions of the message detail interface 1800, refer to the embodiment shown in FIG. 17C. Details are not described herein again.

[00905] S1903: After generating an authentication code A based on the information A, the sending device may obtain a data packet based on the authentication code A and original data, where the value of the information A is X in this case.

[00906] The receiving device cannot receive the previous data packet sent by the sending device, and therefore does not update information B of the receiving device. In addition, the receiving device does not send a success application receipt to the sending device, and therefore the value of the information A of the sending device is still X.

[00907] S1904: The sending device sends the data packet to the receiving device.

[00908] In the inbound process, the sending device is the terminal 100, and the receiving device is the satellite network device 200. After sending the data packet to the satellite network device 200, the terminal 100 may display a message box 1811 and a sending prompt 1812 shown in FIG. 18B. For detailed descriptions of the message box 1811 and the sending prompt 1812, refer to the embodiment shown in FIG. 17C. Details are not described herein again.

[00909] S1905: The receiving device generates an authentication code B based on the information B and the data packet, where a value of the information B is X in this case.

[00910] S1906: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the information B to X+i.

[00911] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet is successfully received. The receiving device may add i to the value of the information B, that is, update the value of the information B to X+i.

[00912] S1907: The receiving device sends a success application receipt to the sending device.

[00913] S1908: The sending device updates the value of the information A to X+i.

[00914] After receiving the success application receipt, the sending device determines that the 2nd data packet is successfully sent. Because the sending device does not update the value of the information A when sending the 2nd data packet, the sending device may determine that the receiving device does not update the value of the information B, either, that is, the receiving device does not receive the 1st data packet. The sending device determines that the 1st data packet fails to

be sent.

[00915] In the inbound process, the sending device is the terminal 100, and the receiving device is the satellite network device 200. After receiving the success application receipt, the terminal 100 may display failure prompt information 2101 and success prompt information 2102 shown in FIG. 20. The failure prompt information 2101 may be used to prompt a user that the terminal 100 fails to send content in a message box 1801 to a recipient. The success prompt information 2102 may be used to prompt the user that the terminal 100 successfully sends content in the message box 1811 to the recipient.

[00916] It should be noted that this application is not limited to the foregoing embodiments, and further provides the following embodiments. It should be noted that the following embodiments may be used in mutual combination with any one or more of the foregoing embodiments.

[00917] In some embodiments, if a sending device has sent at least two data packets before receiving a failure application receipt (the sending device does not receive an application receipt during sending of the at least two data packets), after receiving the failure application receipt, the sending device cannot determine which data packet in the at least two data packets is successfully sent.

[00918] Therefore, in a possible implementation, information A of a sending device is context (context) information A, and information B of a receiving device is context information B. The context information A may indicate information about a quantity of sent data packets. The information B of the receiving device is the context information B, and the context information B may indicate information about a quantity of received data packets. The sending device may add a message ID field A to a data packet. The message ID field A may be used to identify the data packet. The receiving device may determine a value of a message ID field B based on a message ID field A of a successfully received data packet. The receiving device may add the message ID field B to an application receipt. The message ID field B may be used to identify a latest successfully received data packet. The application receipt to which the message ID field B of the successfully received data packet is added may be referred to as an indication application receipt. In this way, when sending a plurality of data packets generated based on a same value of the context information A, the sending device can determine the successfully sent data packet by using the message ID field B in the application receipt.

[00919] A terminal 100 and a satellite network device 200 may obtain context information by using a cellular network, the terminal 100 may obtain context information by using an intermediate device, or the terminal 100 and the satellite network device 200 may preset context information. For detailed descriptions of obtaining the context information by the terminal 100 and the satellite network device 200, refer to the foregoing embodiments. Details are not described herein again.

[00920] It should be noted that in an inbound process, a success application receipt, a failure application receipt, and an indication application receipt may be collectively referred to as a first application receipt. In an outbound process, a success application receipt, a failure application receipt, and an indication application receipt may be collectively referred to as a third application receipt. It may be understood that, in the inbound process, if the satellite network device 200 generates only a success application receipt and a failure application receipt, the success application receipt and the failure application receipt may be collectively referred to as a first application receipt. In the outbound process, if the terminal 100 generates only a success application receipt and a failure application receipt, the success application receipt and the failure application receipt may be collectively referred to as a third application receipt.

[00921] FIG. 21A and FIG. 21B are a schematic diagram of a processing procedure of a transmission method according to an embodiment of this application.

[00922] 1. A sending device generates an authentication code A based on original data and context information A.

[00923] The context information A may indicate information about a quantity of sent data packets. The information about the quantity of sent data packets is information about a quantity of data packets successfully sent by the sending device. Herein, the information about the quantity of successfully sent data packets may be a sum of a preset offset value, a quantity of success application receipts received by the sending device, and a quantity of indication application receipts received by the sending device. The preset offset value is greater than or equal to 0. That is, after receiving a success application receipt/an indication application receipt, the sending device may add a preset value to a value of the context information A. It should be noted that an increment of the context information A is related to the quantity of data packets successfully sent by the sending device.

[00924] The sending device may obtain the authentication code A based on the context information A and the original data. For detailed descriptions of obtaining the authentication code A by the sending device, refer to the foregoing embodiment shown in FIG. 7A and FIG. 7B. Details are not described herein again.

[00925] In a possible implementation, the sending device may generate the authentication code A based on the context information A, a specified key, and the original data, and then generate a data packet based on the authentication code A and the original data. A receiving device may generate an authentication code B based on context information B, the specified key, and the data packet. In this way, validity of the sending device can be verified by using the specified key, thereby ensuring transmission security.

[00926] 2. The sending device obtains the data packet based on a message ID field A, the

original data, and the authentication code A.

[00927] The sending device may concatenate the message ID field A, the authentication code A, and the original data together, to obtain the data packet.

[00928] Specifically, the sending device may store a message ID. When the value of the context information A does not change, a value of the message ID may be updated with a data packet generated by the sending device. That is, the sending device may update the value of the message ID after generating a data packet based on the message ID field A corresponding to the message ID. After the value of the context information A changes, the sending device may reset the value of the message ID. In this way, when the value of the context information A does not change, because the message ID can identify different data packets, the sending device and the receiving device may distinguish between data packets by using message ID fields of the data packets. That is, when the sending device sends a plurality of data packets and does not receive a success application receipt, the receiving device may send a message ID of a latest successfully received data packet to the sending device, so that the sending device can determine a sending status of the plurality of data packets based on a value of the message ID.

[00929] For example, when a length of the message ID is 2 bits, the message ID may be "00", "01", "10", or "11". After generating, based on a message ID "00", a data packet 1 including a message ID field A "00", the sending device may send the data packet 1 to the receiving device, and update a value of the message ID to "01". After the sending device receives a success application receipt of the receiving device, the sending device may update the value of the context information A, and reset the value of the message ID to "00". Then, the sending device may generate and send, to the receiving device, a data packet 2 including a message ID field A "00".

[00930] After generating, based on a message ID "00", a data packet 1 including a message ID field A "00", the sending device may send the data packet 1 to the receiving device, and update a value of the message ID to "01". When the sending device does not receive an application receipt of the data packet 1 whose message ID field A is "00", the sending device may generate and send, to the receiving device, a data packet 2 including a message ID field A "01", and the sending device may further update the value of the message ID to "10". When the sending device does not receive an application receipt of the data packet 2 whose message ID field A is "01", the sending device may generate and send, to the receiving device, a data packet 3 including a message ID field A "10", and the sending device may further update the value of the message ID to "11". After the sending device receives an indication application receipt including a message ID field B "01", the sending device may determine that the data packets whose message ID fields A are "00" and "10" fail to be sent, and the data packet whose message ID field A is "01" is successfully sent. The sending device may update the value of the context information A and adjust the value of the

message ID to "00".

[00931] Optionally, the sending device may add packet header information in front of the authentication code A and the original data that are concatenated together, to obtain the data packet. The packet header information may include the message ID field A and the like.

[00932] In a possible implementation, the sending device may concatenate the authentication code A and the original data together, to obtain concatenated data. Then, the sending device uses the specified key to encrypt the concatenated data by using a specified algorithm, to obtain encrypted data. The sending device may add packet header information in front of the encrypted data. The packet header information includes an encryption indication field and the message ID field A. The encryption indication field may indicate the specified algorithm (for example, an SM3 hash algorithm) used by the sending device. In this way, because the sending device encrypts the data and then sends the encrypted data to the receiving device, data security can be further ensured. Optionally, the sending device may concatenate the message ID field A, the authentication code A, and the original data together, and then perform encryption by using the specified key.

[00933] The sending device may send the data packet to the receiving device. For descriptions of sending the data packet by the sending device to the receiving device during inbound, refer to the foregoing embodiment shown in FIG. 2A(1) and FIG. 2A(2). For descriptions of sending the data packet by the sending device to the receiving device during outbound, refer to the foregoing embodiment shown in FIG. 3A(1) to FIG. 3A(3). Details are not described herein again.

[00934] In a possible implementation, when the sending device is a terminal 100, after the sending device sends the data packet to the receiving device, the sending device may display sending prompt information. The sending prompt information may be used to prompt a user that the sending device has sent a satellite message to the receiving device.

[00935] 3. The receiving device obtains the message ID field A, the authentication code A, and the original data based on the data packet.

[00936] After the receiving device receives the data packet sent by the sending device, the receiving device may extract the message ID field A, the authentication code A, and the original data from the data packet. For descriptions of receiving the data packet by the receiving device during inbound, refer to the foregoing embodiment shown in FIG. 2B(1) and FIG. 2B(2). For descriptions of receiving the data packet by the receiving device during outbound, refer to the foregoing embodiment shown in FIG. 3B(1) to FIG. 3B(3). Details are not described herein again.

[00937] In a possible implementation, the data packet includes the encryption indication field and the encrypted data. The receiving device may decrypt the encrypted data in the data packet based on the encryption indication field and the specified key, to obtain the message ID field A, the authentication code A, and the original data.

[00938] 4. The receiving device generates the authentication code B based on the context information B and the data packet.

[00939] The receiving device may obtain the authentication code B through calculation based on the context information B and the original data in the data packet by using a specified algorithm (for example, the SM3 hash algorithm). The specified algorithm of the receiving device is the same as the specified algorithm of the sending device. For example, the sending device may add a specified algorithm indication to a packet header of the data packet, where the specified algorithm indication may indicate the specified algorithm used by the sending device; and the receiving device may determine, based on the specified algorithm indication in the received data packet, the specified algorithm used by the sending device. For another example, the sending device and the receiving device may negotiate about a used specified algorithm in a cellular network.

[00940] In a possible implementation, when the sending device generates the authentication code A based on the original data, the context information A, and the specified key, the receiving device may generate the authentication code B based on the original data, the context information B, and the specified key. The sending device and the receiving device may preset parameters required for generating the authentication codes.

[00941] 5. The receiving device determines a receiving status of the data packet based on the authentication code B.

[00942] The receiving device may determine the receiving status of the data packet by determining, through comparison, whether the authentication code A is the same as the authentication code B.

[00943] (1) When the authentication code B is the same as the authentication code A, the receiving device determines that the data packet is successfully received. The receiving device may perform a corresponding processing operation on the original data. For specific descriptions, refer to the embodiment in FIG. 7A and FIG. 7B.

[00944] The receiving device may determine a value of a message ID field B based on a value of the message ID field A, and may further update a value of the context information B. Specifically, the receiving device may add a preset value to the value of the context information B.

[00945] The receiving device may further generate a success application receipt and send the success application receipt to the sending device. The success application receipt may indicate that the receiving device successfully receives the data packet.

[00946] (2) When the authentication code B is different from the authentication code A, the receiving device may obtain information C based on the context information B. Specifically, the receiving device may subtract a preset value from a value of the context information B, to obtain the information C. The receiving device may obtain an authentication code C based on the

information C and the original data by using a specified authentication algorithm. The receiving device may determine, through comparison, whether the authentication code C is the same as the authentication code A.

[00947] (3) When the authentication code A is the same as the authentication code C, the receiving device may determine that the data packet fails to be received. The receiving device may further generate and send, to the sending device, an indication application receipt. The indication application receipt includes a message ID field B, and the message ID field B may be used to identify a data packet latest successfully received by the receiving device. Because the authentication code C generated by the receiving device based on the information C is the same as the authentication code A, the receiving device may determine that the sending device does not update the value of the context information A, that is, the receiving device may determine that the sending device does not receive a success application receipt indicating the latest successfully received data packet. The receiving device may generate the indication application receipt indicating the latest successfully received data packet. The indication application receipt may further indicate, to the sending device, that the current data packet fails to be received.

[00948] In a possible implementation, when determining that the authentication code A is the same as the authentication code C, the receiving device may determine that the data packet is successfully received. The receiving device may add the preset value to the value of the context information B, and determine a value of a message ID field B based on the message ID field A of the current data packet. The receiving device may further generate and send, to the sending device, an indication application receipt. The indication application receipt may include a message ID field B of a latest successfully received data packet. The indication application receipt may indicate, to the sending device, that the current data packet and a data packet including a message ID field A that has a same value as the message ID field B are successfully received. The sending device may add the preset value to the value of the context information A twice based on the indication application receipt.

[00949] (4) When the authentication code A is different from the authentication code C, the receiving device may determine that the data packet fails to be received. The receiving device may further generate and send, to the sending device, a failure application receipt. The failure application receipt may indicate that the receiving device fails to receive the data packet.

[00950] For example, an application receipt may include but is not limited to a status code. The application receipt may indicate the receiving status of the data packet by using the status code. Each value of the status code may uniquely correspond to one status of receiving the data packet by the receiving device. For example, the status code of the application receipt and the receiving status corresponding to the status code are shown in Table 1.

Table 1: Application receipt description

Status code	Description
0000	Receiving succeeds
0001	Decryption error
0010	Decoding error
0011-1011	Reserved
1100	Context information mismatch (mismatch), where a data packet with a message ID=00 is correctly transmitted
1101	Context information mismatch (mismatch), where a data packet with a message ID=01 is correctly transmitted
1110	Context information mismatch (mismatch), where a data packet with a message ID=10 is correctly transmitted
1111	Context information mismatch (mismatch), where a data packet with a message ID=11 is correctly transmitted

[00951] For example, a length of the status code may be 4 bits. When the authentication code A is the same as the authentication code B, a value of the status code may be "0000", and the status code may indicate that the data packet is successfully received, that is, an application receipt including the status code "0000" is a success application receipt.

[00952] When the authentication code A is different from the authentication code B, the receiving device may generate the authentication code C. When the authentication code A is different from the authentication code C, a value of the status code may be "0001", and the status code may indicate that the receiving device fails to decrypt the data packet (for example, a decryption failure caused by a key error or a decryption failure caused by an authentication code error), that is, an application receipt including the status code "0001" is a failure application receipt.

[00953] When the authentication code A is the same as the authentication code C, the receiving device may determine that there is a mismatch between context information of the sending device and context information of the receiving device. The first two bits of the status code of the receiving device may be "11", and the last two bits of the status code may be the value of the message ID field B. When a value of the status code is "1100", the status code may indicate that a data packet whose value of a message ID field A is "00" and that is received by the receiving device is successfully received, that is, an application receipt including the status code "1100" is an indication application receipt. When a value of the status code is "1101", the status code may indicate that a data packet whose message ID field A is "01" and that is received by the receiving

device is successfully received, that is, an application receipt including the status code "1101" is an indication application receipt. When a value of the status code is "1110", the status code may indicate that a data packet whose message ID field is "10" and that is received by the receiving device is successfully received, that is, an application receipt including the status code "1110" is an indication application receipt. When a value of the status code is "1111", the status code may indicate that a data packet whose message ID field is "11" and that is received by the receiving device is successfully received, that is, an application receipt including the status code "1111" is an indication application receipt.

[00954] It should be noted that after updating the value of the context information A, the sending device adjusts the value of the message ID associated with the data packet to "00". When the sending device does not receive an application receipt after sending a data packet whose message ID indication A is "00", the sending device may continue to send a data packet whose message ID is "01". If the sending device still does not receive an application receipt, the sending device may continue to send a data packet whose message ID is "10". After the sending device receives a success application receipt/an indication application receipt, the sending device may update the value of the context information A, and adjust the value of the message ID field to "00". The rest can be deduced from this.

[00955] For another example, when the receiving device fails to decode the data packet, and a value of the status code is "0010", the status code may indicate that the receiving device fails to decode the data packet (for example, a decoding failure caused by inconsistent encoding manners between the sending device and the receiving device), that is, an application receipt including the status code "0010" is a failure application receipt. Other values of the status code may be reserved values.

[00956] It should be noted that the foregoing descriptions of the status code are merely an example, the status code may be alternatively a data segment of another length, and the receiving status corresponding to the value of the status code is not limited to the foregoing described case. This is not limited in this application.

[00957] 6. The sending device determines a sending status of the data packet based on an application receipt.

[00958] The sending device may determine the sending status of the data packet based on the application receipt.

[00959] (1) When the application receipt received by the sending device is a success application receipt indicating that the receiving device successfully receives the data packet, the sending device may determine that the data packet is successfully sent. The sending device may add a preset value to the value of the context information A. The preset value added in the sending device

is the same as the preset value added in the receiving device.

[00960] In some embodiments, when the sending device is the terminal 100, after receiving the success application receipt, the sending device may display success prompt information. The success prompt information may be used to prompt the user that the data packet is successfully sent.

[00961] (2) When the application receipt received by the sending device is a failure application receipt indicating that the receiving device fails to receive the data packet, the sending device may determine that the data packet fails to be sent.

[00962] Optionally, the sending device may retransmit the data packet that fails to be sent.

[00963] In some embodiments, when the sending device is the terminal 100, after receiving the failure application receipt, the sending device may display failure prompt information. The failure prompt information may be used to prompt the user that the data packet fails to be sent.

[00964] (3) When the application receipt received by the sending device is an indication application receipt, the sending device may determine that the data packet fails to be sent.

[00965] The sending device may determine a latest successfully sent data packet based on a message ID field B in the indication application receipt. Specifically, the sending device may determine a message ID field A of the latest successfully sent data packet based on the message ID field B in the indication application receipt. The sending device may determine the latest successfully sent data packet based on the message ID field A.

[00966] The sending device may further add a preset value to the value of the context information A. Because the sending device may determine, based on the indication application receipt, that a success application receipt of a data packet that has been successfully sent is not received, the sending device may determine that a data packet has been previously successfully sent, and accordingly update the value of the context information A.

[00967] For example, after the sending device receives an application receipt including a status code "1100", the sending device may determine that a data packet whose message ID field is "00" is successfully sent, and the sending device may update the value of the context information A.

[00968] In some embodiments, when the sending device is the terminal 100, after receiving the indication application receipt, the sending device may display success prompt information and failure prompt information. The success prompt information may be used to prompt the user that the data packet indicated by the message ID field B is successfully sent. The failure prompt information may be used to prompt the user that the current data packet fails to be sent.

[00969] In a possible implementation, the indication application receipt may indicate that the data packet indicated by the message ID field B is successfully sent, and may further indicate that the current data packet is successfully sent. After receiving the indication application receipt, the

sending device may add the preset value to the value of the context information A twice. The sending device may further display success prompt information 1 and success prompt information 2. The success prompt information 1 may be used to prompt the user that the data packet identified by the message ID field B is successfully sent. The success prompt information 2 may be used to prompt the user that the current data packet is successfully sent.

[00970] The following describes an inbound procedure of a transmission method according to an embodiment of this application.

[00971] A terminal 100 may generate a first authentication code based on first information, a specified key, and original data. The first information is first context information, and may indicate information about a quantity of sent data packets. The terminal 100 may obtain a first data packet based on a first message ID, the first authentication code, the specified key, and the original data. The terminal 100 may send the first data packet to a satellite network device 200. After receiving the first data packet, the satellite network device 200 may generate a second authentication code based on second information, the specified key, and the first data packet. The second information is second context information, and indicates information about a quantity of received data packets. The satellite network device 200 may determine a receiving status of the first data packet based on the second authentication code. When the second authentication code is different from the first authentication code, the satellite network device 200 may generate a temporary authentication code. When the first authentication code is the same as the temporary authentication code, the satellite network device 200 may generate an indication application receipt. The indication application receipt includes a second message ID field, and the second message ID field indicates a latest data packet successfully received by the satellite network device 200. In this way, a problem that the receiving device repeatedly receives a same data packet does not occur, and a sending status of the data packet can be further determined after an application receipt is lost.

[00972] FIG. 22A and FIG. 22B are a schematic diagram of an inbound transmission procedure according to an embodiment of this application.

[00973] S2201: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about a key, first information, and second information.

[00974] For descriptions of negotiating about the key, the first information, and the second information by the terminal 100, the satellite network device 200, and the cellular network device 400, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again. After negotiating about the key, both the terminal 100 and the satellite network device 200 store the specified key. The terminal 100 stores the first information. The satellite network device 200 stores the second information. An initial value of the first information is the same as an initial value of the second information.

[00975] S2202: The terminal 100 obtains original data.

[00976] S2203: The terminal 100 generates a first authentication code based on the specified key, the original data, and the first information.

[00977] The terminal 100 may obtain the first authentication code through calculation based on the stored first information, the specified key, and the original data by using a specified authentication algorithm (for example, an SM3 hash algorithm).

[00978] S2204: The terminal 100 may obtain a first data packet based on a first message ID, the first authentication code, and the original data.

[00979] The terminal 100 may generate first indication information (also referred to as a first message ID field) based on the first message ID. The terminal 100 may concatenate the first message ID field, the first authentication code, and the original data, to obtain the first data packet.

[00980] In a possible implementation, the terminal 100 may further encrypt, by using the specified key, the first authentication code and the original data that are concatenated together, to obtain the first data packet. Optionally, the terminal 100 may encrypt, by using the specified key, the first message ID field, the first authentication code, and the original data that are concatenated together, to obtain the first data packet.

[00981] S2205: The terminal 100 sends the first data packet to the satellite network device 200, where the first data packet includes the first message ID field.

[00982] The terminal 100 may update a value of the first message ID after sending the first data packet to the satellite network device 200. For example, the terminal 100 may add a preset value to the value of the first message ID. An updated value of the first message ID is different from the value that is of the first message ID and that exists before the update.

[00983] In a possible implementation, after sending the first data packet to the receiving device, the terminal 100 may display sending prompt information. The sending prompt information may be used to prompt a user that the terminal 100 has sent the first data packet to the satellite network device 200.

[00984] S2206: The satellite network device 200 may generate a second authentication code based on the specified key, the original data, and the second information.

[00985] S2207: The satellite network device 200 determines whether the first authentication code is the same as the second authentication code.

[00986] The satellite network device 200 may determine a receiving status of the first data packet by determining, through comparison, whether the first authentication code is the same as the second authentication code. When the first authentication code is the same as the second authentication code, the satellite network device 200 may perform step S2208 to step S2210.

[00987] Optionally, the satellite network device 200 may further record and forward, to a

network element (for example, a short message service center) in a cellular network, time at which the first data packet is successfully received or the first message ID. The time at which the first data packet is successfully received or the first message ID is used by the network element in the cellular network to record sending success time of an inbound message, to subsequently send the first message ID of transmission success to the terminal 100 in the cellular network, to update a sending status of information for which the terminal 100 fails to receive an application receipt in a satellite network.

[00988] When the first authentication code is different from the second authentication code, the satellite network device 200 may perform step S2213 to step S2215.

[00989] S2208: The satellite network device 200 updates a value of the second information, and determines a value of a second message ID.

[00990] The satellite network device 200 may add a preset value to the value of the second information. For example, when the value of the second information is 0 and the preset value is 1, an updated value of the second information is 1.

[00991] The satellite network device 200 may further determine a value of a second message ID field (also referred to as second indication information) based on the first message ID field of the data packet. The value of the second message ID field is the same as a value of the first message ID field.

[00992] S2209: The satellite network device 200 sends the original data to the cellular network device 400.

[00993] S2210: The satellite network device 200 sends a success application receipt to the terminal 100.

[00994] S2211: The terminal 100 updates a value of the first information.

[00995] After receiving the success application receipt sent by the satellite network device 200, the terminal 100 may add a preset value to the value of the first information. The preset value added for the first information is the same as the preset value added for the second information, in other words, an updated value of the first information is the same as the updated value of the second information. Optionally, the terminal 100 may further perform step S2212.

[00996] S2212: The terminal 100 displays success prompt information.

[00997] The terminal 100 displays the success prompt information. The success prompt information prompts the user that the first data packet is successfully sent.

[00998] S2213: The satellite network device 200 obtains temporary information based on the second information.

[00999] After determining that the first authentication code is different from the second authentication code, the satellite network device 200 may subtract a preset value from a value of

the second information, to obtain the temporary information.

[001000] S2214: The satellite network device 200 generates a temporary authentication code based on the specified key, the original data, and the temporary information.

[001001] The satellite network device 200 may obtain the temporary authentication code through calculation based on the temporary information, the specified key, and the original data by using a specified authentication algorithm (for example, an SM3 hash algorithm).

[001002] S2215: The satellite network device 200 determines whether the first authentication code is the same as the temporary authentication code.

[001003] The satellite network device 200 may determine, through comparison, whether the first authentication code is the same as the temporary authentication code, to determine whether the first information of the terminal 100 is updated, that is, whether the terminal 100 receives a previous success application receipt. When the first authentication code is the same as the temporary authentication code, the satellite network device 200 may perform step S2216.

[001004] When the first authentication code is different from the temporary authentication code, the satellite network device 200 may perform step S2219.

[001005] S2216: The satellite network device 200 sends an indication application receipt (including a second message ID field) to the terminal 100.

[001006] The satellite network device 200 generates the indication application receipt. The indication application receipt includes second indication information (also referred to as the second message ID field), and the second message ID field may indicate a latest successfully received data packet.

[001007] S2217: The terminal 100 updates a value of the first information.

[001008] After receiving the indication application receipt sent by the satellite network device 200, the terminal 100 may add a preset value to the value of the first information. An updated value of the first information is the same as a current value of the second information. Optionally, the terminal 100 may further perform step S2218.

[001009] S2218: The terminal 100 displays success prompt information and failure prompt information.

[001010] The terminal 100 displays the success prompt information and the failure prompt information. The success prompt information prompts that the data packet indicated by a second message ID is successfully sent. The failure prompt information indicates that the first data packet indicated by the first message ID fails to be sent.

[001011] S2219: The satellite network device 200 sends a failure application receipt to the terminal 100.

[001012] Optionally, after receiving the failure application receipt, the terminal 100 may further

perform step S2220.

[001013] S2220: The terminal 100 displays failure prompt information.

[001014] The terminal 100 displays the failure prompt information. The failure prompt information prompts the user that the first data packet fails to be sent.

[001015] For specific descriptions of step S2201 to step S2212, step S2219, and step S2220, refer to the foregoing embodiment shown in FIG. 12. Details are not described herein again.

[001016] The following describes an outbound procedure of another transmission method according to an embodiment of this application.

[001017] A satellite network device 200 may generate a fourth authentication code based on sixth information and original data. The sixth information is sixth context information, and indicates information about a quantity of sent data packets. The satellite network device 200 may obtain a third data packet based on a fourth message ID, the fourth authentication code, and the original data. The satellite network device 200 may send the third data packet to a terminal 100. After receiving the third data packet, the terminal 100 may generate a third authentication code based on fifth information and the third data packet. The fifth information is fifth context information, and indicates information about a quantity of received data packets. The terminal 100 may determine a receiving status of the third data packet based on the third authentication code. When the third authentication code is different from the fourth authentication code, the terminal 100 may generate a temporary authentication code. When determining that the fourth authentication code is the same as the temporary authentication code, the terminal 100 may generate an indication application receipt including a third message ID field. The third message ID field indicates a data packet latest successfully received by the terminal 100. In this way, a problem of repeatedly receiving a same data packet does not occur, and a sending status of the data packet can be further determined after an application receipt is lost.

[001018] FIG. 23A and FIG. 23B are a schematic diagram of an outbound transmission procedure according to an embodiment of this application.

[001019] S2301: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about fifth information and sixth information.

[001020] The terminal 100 stores the fifth information. The satellite network device 200 stores the sixth information. An initial value of the fifth information is the same as an initial value of the sixth information.

[001021] S2302: The satellite network device 200 receives original data sent by the cellular network device 400.

[001022] S2303: The satellite network device 200 receives a service request sent by the terminal 100.

[001023] S2304: The satellite network device 200 generates a fourth authentication code based on the original data and the sixth information.

[001024] The satellite network device 200 may generate the fourth authentication code based on the stored sixth information and the original data.

[001025] S2305: The satellite network device 200 obtains a third data packet based on a fourth message ID, the original data, and the fourth authentication code.

[001026] The fourth message ID indicates the third data packet. The satellite network device 200 may generate a fourth message ID field (also referred to as sixth indication information) based on the fourth message ID. The satellite network device 200 may concatenate the fourth message ID field, the fourth authentication code, and the original data, to obtain the third data packet.

[001027] S2306: The satellite network device 200 sends the third data packet to the terminal 100, where the third data packet includes the fourth message ID field.

[001028] S2307: The terminal 100 obtains a third authentication code based on the third data packet and the fifth information.

[001029] S2308: The terminal 100 determines whether the third authentication code is the same as the fourth authentication code.

[001030] The terminal 100 may determine a receiving status of the third data packet by determining, through comparison, whether the third authentication code is the same as the fourth authentication code. When the third authentication code is the same as the fourth authentication code, the terminal 100 may perform step S2309 to step S2311.

[001031] Optionally, the terminal 100 may further record time at which the third data packet is successfully received or the fourth message ID. The time at which the third data packet is successfully received or the fourth message ID may be used by the terminal 100 to subsequently send the fourth message ID of transmission success to the satellite device 200 or a network element in a second transmission system when the terminal 100 accesses the second transmission system (for example, a cellular network or a WLAN), to update a sending status of information for which an application receipt fails to be received in a satellite network. This avoids a charging problem.

[001032] When the third authentication code is different from the fourth authentication code, the terminal 100 may perform step S2313 to step S2315.

[001033] S2309: The terminal 100 displays receiving prompt information.

[001034] S2310: The terminal 100 updates a value of the fifth information, and determines a value of a third message ID field.

[001035] After determining that the third authentication code is the same as the fourth authentication code, the terminal 100 may update the value of the fifth information. The terminal 100 may add a preset value to the value of the fifth information. For example, when the value of

the fifth information is 0 and the preset value is 1, an updated value of the fifth information is 1.

[001036] The terminal 100 may determine the value of the third message ID field (also referred to as fifth indication information) based on a value of the fourth message ID field. The value of the fourth message ID field is the same as the value of the third message ID field.

[001037] S2311: The terminal 100 sends a success application receipt to the satellite network device 200.

[001038] S2312: The satellite network device 200 updates a value of the sixth information.

[001039] After receiving the success application receipt sent by the terminal 100, the satellite network device 200 may add a preset value to the value of the sixth information. The preset value added for the sixth information is the same as the preset value added for the fifth information, in other words, an updated value of the sixth information is the same as the updated value of the fifth information.

[001040] S2313: The terminal 100 obtains temporary information based on the fifth information.

[001041] After determining that the third authentication code is different from the fourth authentication code, the terminal 100 may subtract a preset value from a value of the fifth information, to obtain the temporary information.

[001042] S2314: The terminal 100 generates a temporary authentication code based on a specified key, the original data, and the temporary information.

[001043] The terminal 100 may obtain the temporary authentication code through calculation based on the temporary information, the specified key, and the original data by using a specified authentication algorithm (for example, an SM3 hash algorithm).

[001044] S2315: The terminal 100 determines whether the fourth authentication code is the same as the temporary authentication code.

[001045] The terminal 100 may determine, through comparison, whether the fourth authentication code is the same as the temporary authentication code, to determine whether the sixth information of the satellite network device 200 is updated, that is, whether the satellite network device 200 receives a previous success application receipt. When the fourth authentication code is the same as the temporary authentication code, the terminal 100 may perform step S2316.

[001046] When the fourth authentication code is different from the temporary authentication code, the terminal 100 may perform step S2318.

[001047] S2316: The terminal 100 sends an indication application receipt (including a third message ID field) to the satellite network device 200.

[001048] The terminal 100 generates the indication application receipt. The indication application receipt includes the third message ID field, and the third message ID field indicates a latest successfully received data packet.

[001049] S2317: The satellite network device 200 updates a value of the sixth information.

[001050] After receiving the indication application receipt sent by the terminal 100, the satellite network device 200 may determine that the data packet indicated by a third message ID is successfully sent. The satellite network device 200 may add a preset value to the value of the sixth information. An updated value of the sixth information is the same as a current value of the fifth information.

[001051] S2318: The terminal 100 sends a failure application receipt to the satellite network device 200.

[001052] For specific descriptions of step S2301 to step S2312, step S2317, and step S2318, refer to the foregoing embodiment shown in FIG. 13. Details are not described herein again.

[001053] The following describes the foregoing possible implementation with reference to a scenario. Details are shown in FIG. 24A and FIG. 24B.

[001054] S2401: A sending device obtains a data packet 1 based on a message ID, context information A, and original data, where a value of the context information A is X, and a value of the message ID is y1.

[001055] The sending device may generate an authentication code A based on the context information A. The sending device may obtain a message ID field A based on the stored message ID. The sending device may obtain the data packet 1 based on the message ID field A, the original data, and the authentication code A.

[001056] S2402: The sending device sends the data packet 1 to a receiving device, where the data packet 1 includes the message ID field A and the authentication code A.

[001057] After sending the data packet 1 to the receiving device, the sending device may update the value of the message ID to y2. y1 is different from y2.

[001058] For example, when a length of the message ID is 2 bits, y1 may be "00", and y2 may be "01". In an inbound process, the sending device is a terminal 100, and the receiving device is a satellite network device 200. After sending the data packet 1 including a message ID field A "00" to the satellite network device 200, the terminal 100 may display a message detail interface 2500 shown in FIG. 25A. The message detail interface 2500 may include a message box 2501 and a sending prompt 2502. The message box 2501 may be used to display content of a satellite message that has been sent by the terminal 100 to the satellite network device 200. Herein, the message box 2501 displays "X (00)". The sending prompt 2502 may be used to prompt a user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message box 2501. For specific descriptions of the message detail interface 2500, refer to the embodiment shown in FIG. 15D. Details are not described herein again. The terminal 100 may update the value of the message ID to "01" after generating a data packet based on the current message ID field A.

[001059] S2403: The receiving device generates an authentication code B based on context information B and the data packet 1, where a value of the context information B is X.

[001060] S2404: The receiving device determines that the authentication code A is the same as the authentication code B, updates the value of the context information B to X+i, and determines that a value of a message ID field B is y1.

[001061] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet is successfully received. The receiving device may add i to the value of the information B, that is, update the value of the information B to X+i.

[001062] The receiving device may determine the value of the message ID field B based on a value of the message ID field A of the data packet 1, that is, determine that the value of the message ID field B is y1.

[001063] S2405: The receiving device sends a success application receipt to the sending device.

[001064] S2406: The sending device updates the value of the context information A to X+i.

[001065] The sending device may further adjust the value of the message ID to y1.

[001066] For example, in the inbound process, after receiving the success application receipt, the terminal 100 may display a success prompt 2511 shown in FIG. 25B. The success prompt 2511 may be used to prompt the user that the terminal 100 successfully sends the content displayed in the message box 2501. For specific descriptions of a message detail interface 2500, refer to the embodiment shown in FIG. 15D. Details are not described herein again.

[001067] S2407: The sending device obtains a data packet 2 based on the message ID, the context information A, and original data, where the value of the context information A is X+i, and the value of the message ID is y1.

[001068] S2408: The sending device sends the data packet 2 to the receiving device, where the data packet 2 includes a message ID field A and an authentication code A.

[001069] After sending the data packet 2 to the receiving device, the sending device may update the value of the message ID to y2. y1 is different from y2.

[001070] In the inbound process, after sending the data packet to the satellite network device 200, the terminal 100 may display a message box 2521 and a sending prompt 2522 shown in FIG. 25C. The message box 2521 may be used to display content of a satellite message that has been sent by the terminal 100 to the satellite network device 200. Herein, the message box 2521 displays "X+1 (00)". The sending prompt 2522 may be used to prompt the user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message box 2521. For specific descriptions of a message detail interface 2500, refer to the embodiment shown in FIG. 15D. Details are not described herein again.

[001071] S2409: The receiving device generates an authentication code B based on the context information B and the data packet 2, where the value of the context information B is X+i.

[001072] S2410: The receiving device determines that the authentication code A is the same as the authentication code B, updates the value of the context information B to X+2i, and determines that a value of a message ID field B is y1.

[001073] The receiving device may determine the value of the message ID field B based on a value of the message ID field A of the data packet 2, that is, determine that the value of the message ID field B is y1.

[001074] S2411: The receiving device sends a success application receipt to the sending device.

[001075] S2412: The sending device updates the value of the context information A to X+2i.

[001076] The sending device may further adjust the value of the message ID to y1.

[001077] After receiving the success application receipt, the terminal 100 may display success prompt information 2531 shown in FIG. 25D. The success prompt information 2531 may be used to prompt the user that the terminal 100 successfully sends the content in the message box 2521 to a recipient. The success prompt information 2531 may include but is not limited to text prompt information. For example, the success prompt information 2531 may include text prompt information "Sending succeeds".

[001078] The following describes, with reference to a scenario, a case in which data may be lost in a sending process in embodiments of this application.

[001079] 1. Case in which a data packet is lost.

[001080] When a sending device sends a data packet to a receiving device, and the receiving device does not receive the data packet of the sending device, transmission of a next data packet between the sending device and the receiving device is not affected. This is shown in FIG. 26.

[001081] S2601: A sending device obtains a data packet 1 based on a message ID, context information A, and original data, where a value of the context information A is X, and a value of the message ID is y1.

[001082] The sending device may generate an authentication code A based on the context information A. The sending device may obtain a message ID field A based on the stored message ID. The sending device may obtain the data packet 1 based on the message ID field A, the original data, and the authentication code A.

[001083] S2602: The sending device fails to send the data packet 1 (including the message ID field A and the authentication code A) to a receiving device.

[001084] After sending the data packet 1 to the receiving device, the sending device may update the value of the message ID to y2. y1 is different from y2. For detailed descriptions of the message ID, refer to the foregoing embodiment shown in FIG. 21A and FIG. 21B. Details are not described

herein again.

[001085] The data packet 1 is lost during sending, and therefore the receiving device cannot receive the data packet 1.

[001086] S2603: The sending device obtains a data packet 2 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y2.

[001087] The receiving device cannot receive the data packet 1 sent by the sending device, and therefore does not update context information B of the receiving device. In addition, the receiving device does not send a success application receipt to the sending device, and therefore the value of the context information A of the sending device is still X.

[001088] S2604: The sending device sends the data packet 2 (including a message ID field A and an authentication code A) to the receiving device.

[001089] After sending the data packet 2 to the receiving device, the sending device may update the value of the message ID to y3. y3 is different from y2, and y3 is different from y1.

[001090] The data packet 2 is lost during sending, and therefore the receiving device cannot receive the data packet 2.

[001091] S2605: The sending device obtains a data packet 3 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y3.

[001092] The receiving device cannot receive the data packet 2 sent by the sending device, and therefore does not update the context information B of the receiving device. In addition, the receiving device does not send a success application receipt to the sending device, and therefore the value of the context information A of the sending device is still X.

[001093] S2606: The sending device sends the data packet 3 (including a message ID field A and an authentication code A) to the receiving device.

[001094] After sending the data packet 3 to the receiving device, the sending device may update the value of the message ID to y4. y4 is different from y3, y2, and y1.

[001095] For example, in an inbound process, after sending the data packet 3 to a satellite network device 200, a terminal 100 may display a message detail interface 2700 shown in FIG. 27A. The message detail interface 2700 may include a message box 2701, a message box 2703, a message box 2705, a sending prompt 2702, a sending prompt 2704, and a sending prompt 2706. The message box 2701, the message box 2703, and the message box 2705 may be used to display content of satellite messages that have been sent by the terminal 100 to the satellite network device 200. For example, the message box 2701 displays message content "X (00)" entered by a user, the message box 2703 displays message content "X (01)" entered by the user, and the message box

2705 displays message content "X (10)" entered by the user.

[001096] The sending prompt 2702, the sending prompt 2704, and the sending prompt 2706 may be used to prompt the user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message boxes. For specific descriptions of the message detail interface 2700, refer to the embodiment shown in FIG. 15D. Details are not described herein again.

[001097] S2607: The receiving device generates an authentication code B based on the context information B and the data packet 3, where a value of the context information B is X.

[001098] S2608: The receiving device determines that the authentication code A is the same as the authentication code B, updates the value of the context information B to X+i, and determines that a value of a message ID field B is y3.

[001099] The receiving device determines that the authentication code A is the same as the authentication code B, and determines that the data packet 3 is successfully received. The receiving device may add i to the value of the context information B, that is, update the value of the information B to X+i.

[001100] The receiving device may determine the value of the message ID field B based on a value of the message ID field A in the data packet 3.

[001101] S2609: The receiving device sends a success application receipt to the sending device.

[001102] S2610: The sending device updates the value of the context information A to X+i.

[001103] The sending device may adjust the value of the message ID of the sending device to y1 after receiving the success application receipt. In this way, the sending device can determine a unique data packet based on both the context information A and a value of a message ID field A, so that a length of the message ID can be reduced, thereby saving an air interface resource used for transmission.

[001104] For example, in the inbound process, after receiving the success application receipt, the terminal 100 may display failure prompt information 2711, failure prompt information 2712, and success prompt information 2713 shown in FIG. 27B. The failure prompt information 2711 may be used to prompt the user that the terminal 100 fails to send the content in the message box 2701 to a recipient. The failure prompt information 2712 may be used to prompt the user that the terminal 100 fails to send the content in the message box 2703 to the recipient. The success prompt information 2713 may be used to prompt the user that the terminal 100 successfully sends the content in the message box 2705 to the recipient.

[001105] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again.

[001106] In this way, when the sending device sends a data packet to the receiving device, the data packet is lost in a sending process, and therefore the receiving device cannot receive the data

packet. However, because neither context information of the sending device nor context information of the receiving device is updated, transmission of a subsequent data packet is not affected.

[001107] 2. Case in which an application receipt is lost.

[001108] When a sending device sends a plurality of data packets to a receiving device, after successfully receiving a data packet in the plurality of data packets, the receiving device may update a value of context information B. The receiving device may further determine a value of a message ID field B based on a message ID field A of the successfully received data packet, and send a success application receipt to the sending device.

[001109] The success application receipt sent by the receiving device to the sending device is lost in a sending process, and therefore the sending device cannot receive the success application receipt, and does not update a value of context information A. The sending device sends, to the receiving device, a data packet that is generated based on the un-updated context information A and that includes an authentication code A.

[001110] When determining that authentication codes are different, the receiving device may generate an authentication code C based on the context information B. When determining that the authentication code A is the same as the authentication code C, the receiving device may determine that the sending device does not receive the success application receipt. The receiving device may generate an indication application receipt (which may indicate a latest successfully received data packet) including the message ID field B, and send the indication application receipt to the sending device.

[001111] In this way, the sending device can determine, based on the indication application receipt, the successfully sent data packet and a data packet that fails to be sent, and may update the value of the context information A based on the indication application receipt, without affecting transmission of a subsequent data packet. Details are shown in FIG. 28A and FIG. 28B.

[001112] S2801: A sending device obtains a data packet 1 based on a message ID, context information A, and original data, where a value of the context information A is X, and a value of the message ID is y1.

[001113] S2802: The sending device sends a data packet 1 (including a message ID field A and an authentication code A) to a receiving device.

[001114] After sending the data packet 1 to the receiving device, the sending device may update the value of the message ID to y2. y1 is different from y2. For detailed descriptions of the message ID, refer to the foregoing embodiment shown in FIG. 21A and FIG. 21B. Details are not described herein again.

[001115] The data packet 1 is lost during sending, and therefore the receiving device cannot

receive the data packet 1.

[001116] S2803: The sending device obtains a data packet 2 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y2.

[001117] The receiving device cannot receive the data packet 1 sent by the sending device, and therefore does not update context information B of the receiving device. In addition, the receiving device does not send a success application receipt to the sending device, and therefore the value of the context information A of the sending device is still X.

[001118] S2804: The sending device sends the data packet 2 (including a message ID field A and an authentication code A) to the receiving device.

[001119] After sending the data packet 2 to the receiving device, the sending device may update the value of the message ID to y3. y3 is different from y2 and y1.

[001120] S2805: The receiving device generates an authentication code B based on the context information B and the data packet 2, where a value of the context information B is X.

[001121] S2806: The receiving device determines that the authentication code A is the same as the authentication code B, updates the value of the context information B to X+i, and determines that a value of a message ID field B is y2.

[001122] S2807: The receiving device fails to send a success application receipt to the sending device.

[001123] The success application receipt is lost during sending, and therefore the sending device cannot receive the success application receipt.

[001124] S2808: The sending device obtains a data packet 3 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y3.

[001125] The sending device cannot receive the success application receipt sent by the receiving device, and therefore cannot determine a sending status of the data packet 2, and cannot update the context information A. Therefore, the value of the context information A is still X.

[001126] S2809: The sending device sends the data packet 3 (including a message ID field A and an authentication code A) to the receiving device.

[001127] After sending the data packet 3 to the receiving device, the sending device may update the value of the message ID to y4. y4 is different from y3, y2, and y1.

[001128] For example, in an inbound process, after sending the data packet 3 to a satellite network device 200, a terminal 100 may display a message detail interface 2700 shown in FIG. 27A. For detailed descriptions of the message detail interface 2700, refer to the foregoing embodiment shown in FIG. 26. Details are not described herein again.

[001129] S2810: The receiving device generates an authentication code B based on the context information B and the data packet 3, where the value of the context information B is X+i.

[001130] S2811: The receiving device determines that the authentication code A is different from the authentication code B, and generates an authentication code C.

[001131] After determining that the authentication code A is different from the authentication code B, the receiving device may generate context information C based on the context information B, and generate the authentication code C based on the context information C. The context information B is greater than the context information C by a preset value.

[001132] S2812: The receiving device determines that the authentication code A is the same as the authentication code C, and generates an indication application receipt (including an indication ID field B, where a value of the indication ID field B is y2).

[001133] After determining that the authentication code A is the same as the authentication code C, the receiving device may determine that the value of the context information A of the sending device is different from the value of the context information B, and the receiving device may generate the indication application receipt based on the message ID field B. The value of the message ID field B is y2, and the message ID field B may indicate the data packet 2 latest successfully received by the receiving device.

[001134] S2813: The receiving device sends the indication application receipt to the sending device.

[001135] S2814: The sending device updates the value of the context information A to X+i.

[001136] After receiving the indication application receipt, the sending device may determine, based on the indication application receipt, that the data packet 2 indicated by the message ID field B is successfully sent. The sending device may update the value of the context information A to X+i. The sending device may further adjust the value of the message ID to y1.

[001137] For example, in the inbound process, after receiving the indication application receipt, the terminal 100 may display failure prompt information 2901, success prompt information 2902, and failure prompt information 2903 shown in FIG. 29. The failure prompt information 2901 may be used to prompt a user that the terminal 100 fails to send the content in the message box 2701 to a recipient. The success prompt information 2902 may be used to prompt the user that the terminal 100 successfully sends the content in the message box 2703 to the recipient. The failure prompt information 2903 may be used to prompt the user that the terminal 100 fails to send the content in the message box 2705 to the recipient.

[001138] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again.

[001139] In this way, the sending device can determine the successfully sent data packet by using

the indication application receipt, and update the value of the context information A, so that the sending device and the receiving device can continue to transmit a subsequent data packet.

[001140] However, due to limitation of a length of a message ID field A, when a sending device sends a plurality of data packets that include a same message ID field A and that are generated based on a same value of context information A, if a quantity of data packets indicated by a message ID field B in an indication application receipt received by the sending device is greater than 1, the sending device cannot determine sending statuses of the data packets. This is shown in FIG. 30A and FIG. 30B.

[001141] S3001: A sending device obtains a data packet 1 based on a message ID, context information A, and original data, where a value of the context information A is X, and a value of the message ID is y1.

[001142] S3002: The sending device sends the data packet 1 (including a message ID field A and an authentication code A) to a receiving device.

[001143] After sending the data packet 1 to the receiving device, the sending device may update the value of the message ID to y2. y1 is different from y2. For detailed descriptions of the message ID, refer to the foregoing embodiment shown in FIG. 21A and FIG. 21B. Details are not described herein again.

[001144] S3003: The receiving device generates an authentication code B based on context information B and the data packet 1, where a value of the context information B is X.

[001145] S3004: The receiving device determines that the authentication code A is the same as the authentication code B, updates the value of the context information B to X+i, and determines that a value of a message ID field B is y1.

[001146] S3005: The receiving device fails to send a success application receipt to the sending device.

[001147] The success application receipt is lost during sending, and therefore the sending device cannot receive the success application receipt.

[001148] S3006: The sending device obtains a data packet 2 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y2.

[001149] Because the sending device does not receive the success application receipt, the value of the context information A of the sending device is still X.

[001150] S3007: The sending device sends the data packet 2 (including a message ID field A and an authentication code A) to the receiving device.

[001151] After sending the data packet 2 to the receiving device, the sending device may update the value of the message ID to y3. y3 is different from y2 and y1.

[001152] S3008: The receiving device generates an authentication code B based on the context information B and the data packet 2, where the value of the context information B is X+i.

[001153] S3009: The receiving device determines that the authentication code A is different from the authentication code B, and generates an authentication code C.

[001154] After determining that the authentication code A is different from the authentication code B, the receiving device may generate context information C based on the context information B, and generate the authentication code C based on the context information C. The context information B is greater than the context information C by a preset value, that is, a value of the context information C is X.

[001155] S3010: The receiving device determines that the authentication code A is the same as the authentication code C, and generates an indication application receipt (including an indication ID field B, where a value of the indication ID field B is y1).

[001156] After determining that the authentication code A is the same as the authentication code C, the receiving device may determine that the value of the context information A of the sending device is different from the value of the context information B, and the receiving device may generate the indication application receipt based on the message ID field B. The value of the message ID field B is y1, and the message ID field B may indicate the data packet 1 latest successfully received by the receiving device.

[001157] S3011: The receiving device fails to send the indication application receipt to the sending device.

[001158] The indication application receipt is lost during sending, and therefore the sending device cannot receive the indication application receipt.

[001159] S3012: The sending device obtains a data packet 3 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y3.

[001160] The sending device cannot receive the indication application receipt sent by the receiving device, and therefore cannot determine a sending status of the data packet 2, and cannot update the context information A. Therefore, the value of the context information A is still X.

[001161] S3013: The sending device fails to send the data packet 3 (including a message ID field A and an authentication code A) to the receiving device.

[001162] After sending the data packet 3 to the receiving device, the sending device may update the value of the message ID to y4. y4 is different from y3, y2, and y1.

[001163] The data packet 3 is lost in a sending transmission process, and therefore the receiving device cannot receive the data packet 3.

[001164] S3014: The sending device obtains a data packet 4 based on the message ID, the context

information A, and original data, where the value of the context information A is X, and the value of the message ID is y4.

[001165] The sending device cannot receive an application receipt sent by the receiving device, and therefore cannot determine a sending status of the data packet 3, and cannot update the context information A. Therefore, the value of the context information A is still X.

[001166] S3015: The sending device fails to send the data packet 4 (including a message ID field A and an authentication code A) to the receiving device.

[001167] After sending the data packet 4 to the receiving device, the sending device may update the value of the message ID to y1. Because the sending device presets the value of the message ID to only y1, y2, y3, and y4, after the sending device generates more than four data packets based on the context information A that is X, the sending device may update the value of the message ID to y1 after generating and sending the fourth data packet.

[001168] The data packet 4 is lost in a sending transmission process, and therefore the receiving device cannot receive the data packet 4.

[001169] S3016: The sending device obtains a data packet 5 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y1.

[001170] The sending device cannot receive an application receipt sent by the receiving device, and therefore cannot determine a sending status of the data packet 4, and cannot update the context information A. Therefore, the value of the context information A is still X.

[001171] S3017: The sending device fails to send the data packet 5 (including a message ID field A and an authentication code A) to the receiving device.

[001172] After sending the data packet 5 to the receiving device, the sending device may update the value of the message ID to y2. Because the sending device presets the value of the message ID to only y1, y2, y3, and y4, after the sending device generates more than four data packets based on the context information A that is X, the sending device may update the value of the message ID to y2 after generating and sending the fifth data packet.

[001173] The data packet 5 is lost in a sending transmission process, and therefore the receiving device cannot receive the data packet 5.

[001174] S3018: The sending device obtains a data packet 6 based on the message ID, the context information A, and original data, where the value of the context information A is X, and the value of the message ID is y2.

[001175] The sending device cannot receive an application receipt sent by the receiving device, and therefore cannot determine a sending status of the data packet 5, and cannot update the context information A. Therefore, the value of the context information A is still X.

[001176] S3019: The sending device sends the data packet 6 (including a message ID field A and an authentication code A) to the receiving device.

[001177] After sending the data packet 6 to the receiving device, the sending device may update the value of the message ID to y3. Because the sending device presets the value of the message ID to only y1, y2, y3, and y4, after the sending device generates more than four data packets based on the context information A that is X, the sending device may update the value of the message ID to y3 after generating and sending the sixth data packet.

[001178] For example, in an inbound process, after sending the data packet 6 to a satellite network device 200, a terminal 100 may display a message detail interface 3100 shown in FIG. 31A. The message detail interface 3100 may include a message box 3101, a sending prompt 3102, a message box 3103, a sending prompt 3104, a message box 3105, a sending prompt 3106, a message box 3107, a sending prompt 3108, a message box 3109, a sending prompt 3110, a message box 3111, and a sending prompt 3112. The message box 3101, the message box 3103, the message box 3105, the message box 3107, the message box 3109, and the message box 3111 may be used to display content of satellite messages that have been sent by the terminal 100 to the satellite network device 200. For example, the message box 3101 displays message content "X (00)" entered by a user, the message box 3103 displays message content "X (01)" entered by the user, the message box 3105 displays message content "X (10)" entered by the user, the message box 3107 displays message content "X (11)" entered by the user, the message box 3109 displays message content "X (00)" entered by the user, and the message box 3111 displays message content "X (01)" entered by the user.

[001179] The sending prompt 3102, the sending prompt 3104, the sending prompt 3106, the sending prompt 3108, the sending prompt 3110, and the sending prompt 3112 may be used to prompt the user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message boxes. For detailed descriptions of the message detail interface 3100, refer to the embodiment shown in FIG. 26. Details are not described herein again.

[001180] S3020: The receiving device generates an authentication code B based on the context information B and the data packet 6, where the value of the context information B is X+i.

[001181] S3021: The receiving device determines that the authentication code A is different from the authentication code B, and generates an authentication code C.

[001182] After determining that the authentication code A is different from the authentication code B, the receiving device may generate context information C based on the context information B, and generate the authentication code C based on the context information C. The context information B is greater than the context information C by a preset value, that is, a value of the context information C is X.

[001183] S3022: The receiving device determines that the authentication code A is the same as the authentication code C, and generates an indication application receipt (including an indication ID field B, where a value of the indication ID field B is y1).

[001184] After determining that the authentication code A is the same as the authentication code C, the receiving device may determine that the value of the context information A of the sending device is different from the value of the context information B, and the receiving device may generate the indication application receipt based on the message ID field B. The value of the message ID field B is y1, and the message ID field B may indicate the data packet 1 latest successfully received by the receiving device.

[001185] S3023: The receiving device sends the indication application receipt to the sending device.

[001186] S3024: The sending device updates the value of the context information A to X+i.

[001187] After receiving the indication application receipt, the sending device may update the value of the context information A to X+i.

[001188] The sending device determines, based on the message ID field B in the indication application receipt, that a data packet whose message ID field A is y1 is successfully received. However, because the data packet whose message ID field A is y1 includes the data packet 1 and the data packet 5, the sending device cannot determine a successfully sent data packet.

[001189] For example, in the inbound process, after receiving the indication application receipt, the terminal 100 may display failure prompt information 3113, failure prompt information 3114, failure prompt information 3115, and failure prompt information 3116 shown in FIG. 31B. The failure prompt information 3111 may be used to prompt the user that the terminal 100 fails to send the content in the message box 3103 to a recipient. The failure prompt information 3112 may be used to prompt the user that the terminal 100 fails to send the content in the message box 3105 to the recipient. The failure prompt information 3113 may be used to prompt the user that the terminal 100 fails to send the content in the message box 3107 to the recipient. The failure prompt information 3114 may be used to prompt the user that the terminal 100 fails to send the content in the message box 3111 to the recipient.

[001190] It should be noted that the sending device cannot determine sending statuses of the data packet 1 and the data packet 5, and therefore still displays the sending prompt 3102 and the sending prompt 3110.

[001191] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again.

[001192] Therefore, in a possible implementation, after a sending device and a receiving device return from a satellite network to a cellular network, the receiving device may send a set

application receipt (also referred to as a second application receipt) to the sending device. The set application receipt may indicate a data packet successfully received by the receiving device. The set application receipt may include identification information of the data packet successfully received by the receiving device (for example, the identification information may include but is not limited to a message ID field, receiving time of the data packet, context information, and the like). The sending device may determine the successfully sent data packet based on the identification information of the data packet in the set application receipt.

[001193] This application is not limited to the foregoing embodiments, and further provides the following embodiments. It should be noted that the following embodiments may be used in mutual combination with any one or more of the foregoing embodiments.

[001194] In a possible implementation, information A of a sending device is context information A, and information B of a receiving device is context information B. The context information A may indicate a count value or a sequence number of a data packet sent by the sending device. The context information B may indicate a count value or a sequence number of a data packet received by the receiving device. In this way, after the receiving device receives a repeatedly sent data packet, because a count value or a sequence number of the received data packet changes, the receiving device can update a value of context information B. Because an updated value of the context information B is different from a value of context information A in the repeated data packet, the receiving device cannot parse the repeated data packet, so that problems of repeated processing and charging do not occur. In addition, because the sending device updates the value of the context information A based on a quantity of sent data packets, even if the sending device does not receive a success application receipt of the receiving device, the sending device updates the value of the context information A, and generates a new data packet based on an updated value of the context information A, without affecting parsing of the receiving device for the new data packet.

[001195] In some embodiments, when context information indicates a count value of a data packet, an initial value of the context information A of the sending device is greater than an initial value of the context information B of the receiving device by a preset value. The sending device may generate a data packet based on the context information A. After sending, to the receiving device, the data packet including an authentication code A, the sending device may add the preset value to the value of the context information A. After receiving the data packet, the receiving device may add the preset value to the value of the context information B. The receiving device may generate an authentication code B based on the context information B, and determine a receiving status of the data packet based on the authentication code B.

[001196] For example, a length of the context information A and a length of the context information B may be 5 bits. The initial value of the context information A may be "00001", the

initial value of the context information B may be "00000", and the sending device may generate a data packet 1 based on the context information A "00001". After sending the data packet 1 to the receiving device, the sending device may update the value of the context information A to "00010". After receiving the data packet 1, the receiving device may update the value of the context information B to "00001", and the receiving device may generate an authentication code B based on the context information B "00001". Then, the sending device may generate a data packet 2 based on the context information A "00010", and update the value of the context information A to "00011" after sending the data packet 2 to the receiving device. After receiving the data packet 2, the receiving device may update the value of the context information B to "00010", and the receiving device may generate an authentication code B based on the context information B "00010". The rest can be deduced from this.

[001197] In this way, the receiving device does not perform repeated processing.

[001198] In some embodiments, context information indicates a sequence number of a data packet. The context information A of the sending device includes a hyper frame number (hyper frame number, HFN) A and a sequence number (sequence number) A. The sending device may generate, based on the sequence number A, a data packet including a sequence number field A and an authentication code A, and send the data packet to the receiving device in a first transmission system. The receiving device may determine a value of a hyper frame number B based on the sequence number field A in the data packet, and obtain the context information B based on the sequence number field A and the hyper frame number B. The receiving device may generate an authentication code B based on the context information B and the data packet, and determine a receiving status of the data packet based on the authentication code B. Because a data length of the sequence number field A is limited, a value of the sequence number field A returns to an initial value as the value of the sequence number field A is updated. When an updated value of the sequence number A of the sending device is less than a value that is of the sequence number A and that exists before an update, the sending device updates a value of the hyper frame number A, that is, adds a preset value to the value of the hyper frame number A. When the value of the sequence number field A received by the receiving device is less than or equal to a value of a sequence number B, the receiving device may update the value of the hyper frame number B, that is, add the preset value to the value of the hyper frame number B. After updating the value of the hyper frame number B, the receiving device may update the value of the sequence number B to the value of the sequence number field A.

[001199] For example, a length of the context information A and a length of the context information B may be 5 bits. The sending device may store the context information A, and an initial value of the context information A may be "00000". In the context information A, the hyper

frame number A is "0000", and the sequence number A is "0". The receiving device may store the context information B. In the context information B, an initial value of the hyper frame number B may be "0000", and an initial value of the sequence number B is smaller than an initial value of the sequence number A.

[001200] The sending device may generate a data packet 1 including the sequence number field A "0". After sending the data packet 1 to the receiving device, the sending device may update the value of the context information A to "00001". After receiving the data packet 1, the receiving device may determine, based on the sequence number field A, that the value of the hyper frame number B remains unchanged and is still "0000". The receiving device may update the value of the sequence number B to "0". The receiving device may concatenate the hyper frame number B and the sequence number field A, to obtain context information B "00000".

[001201] Then, the sending device may generate, based on the context information A "00001", a data packet 2 including a sequence number field A "1". After sending the data packet 2 to the receiving device, the sending device may update the value of the context information A to "00010". After receiving the data packet 2, the receiving device may determine, based on the sequence number field A, that the value of the hyper frame number B remains unchanged and is still "0000". The receiving device may update the value of the hyper frame number B to "1". The receiving device may concatenate the hyper frame number B and the sequence number field A, to obtain context information B "00001".

[001202] Then, the sending device may generate, based on the context information A "00010", a data packet 3 including a sequence number field A "0". After sending the data packet 3 to the receiving device, the sending device may update the value of the context information A to "00011". After receiving the data packet 3, because the value "0" of the sequence number field A is less than the value "1" of the sequence number B, the receiving device may determine, based on the sequence number field A "0", that the value of the hyper frame number B is changed to "0001". The receiving device may update the value of the hyper frame number B to "0". The receiving device may concatenate the hyper frame number B and the sequence number field A, to obtain context information B "00010". The rest can be deduced from this.

[001203] In this way, when context information indicates a sequence number of a data packet, the receiving device may determine a hyper frame number based on a sequence number in a data packet. Therefore, if the 1st data packet sent by the sending device is lost in a sending process, the receiving device can also determine a hyper frame number based on a sequence number of the 2nd data packet sent by the sending device, and can still successfully parse out the 2nd data packet.

[001204] In this way, when the receiving device does not receive the data packet 2, the receiving device can also update the hyper frame number B to "0001" based on the sequence number A of

the data packet 3, and the receiving device can successfully parse the data packet 3. When the sending device does not receive an application receipt, the sending device may update the value of the context information A with a sent data packet, and the sending device may continue to send a next data packet. It is ensured that the receiving device does not process a repeatedly sent data packet, and data can be continued to be transmitted after a data packet is lost or an application receipt is lost.

[001205] For a manner in which a terminal 100 and a satellite network device 200 obtain an initial value of context information/a hyper frame number, refer to the foregoing embodiments. Details are not described herein again.

[001206] The following describes an inbound procedure of another transmission method according to an embodiment of this application.

[001207] In a possible implementation, in an inbound process, a terminal 100 may generate a first authentication code based on first information, a specified key, and original data. The first information is first context information, and indicates a sequence number of a first data packet. The terminal 100 may obtain, based on the first sequence number, the first authentication code, the specified key, and the original data, the first data packet including first indication information (also referred to as a first sequence number field). The terminal 100 may send the first data packet to a satellite network device 200. After receiving the first data packet, the satellite network device 200 may determine second information based on the first sequence number field, and generate a second authentication code based on the second information, the specified key, and the first data packet. The second information is second context information, and indicates a sequence number of the first data packet. The satellite network device 200 may determine a receiving status of the first data packet based on the second authentication code. In this way, a problem that the satellite network device 200 repeatedly receives a same data packet does not occur, and a next data packet can be further continued to be transmitted after an application receipt/a data packet is lost.

[001208] FIG. 32 is a schematic diagram of an inbound transmission procedure according to an embodiment of this application.

[001209] S3201: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about a key, first information, and second information.

[001210] For descriptions of negotiating about the key, the first information, and the second information by the terminal 100, the satellite network device 200, and the cellular network device 400, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again. After negotiating about the key, both the terminal 100 and the satellite network device 200 store the specified key. The terminal 100 stores a first sequence number and a first hyper frame number in the first information. The satellite network device 200 stores a second hyper frame

number and a second sequence number in the second information. An initial value of the first hyper frame number in the first information is the same as an initial value of the second hyper frame number. An initial value of the first sequence number in the first information is greater than an initial value of the second sequence number in the second information.

[001211] S3202: The terminal 100 obtains original data.

[001212] S3203: The terminal 100 generates a first authentication code based on the specified key, the original data, and the first information.

[001213] The terminal 100 may obtain the first authentication code through calculation based on the stored first information, the specified key, and the original data by using a specified authentication algorithm (for example, an SM3 hash algorithm).

[001214] S3204: The terminal 100 may obtain a first data packet based on the first sequence number, the first authentication code, and the original data.

[001215] The first information of the terminal 100 includes the first hyper frame number and the first sequence number. The terminal 100 may generate first indication information (also referred to as a first sequence number field) based on the first sequence number. A value of the first sequence number field is the same as a value of the first sequence number. The terminal 100 may concatenate the first sequence number field, the first authentication code, and the original data, to obtain the first data packet.

[001216] In a possible implementation, the terminal 100 may further encrypt, by using the specified key, the first authentication code and the original data that are concatenated together, to obtain the first data packet. Optionally, the terminal 100 may encrypt, by using the specified key, the first sequence number field, the first authentication code, and the original data that are concatenated together, to obtain the first data packet.

[001217] S3205: The terminal 100 sends the first data packet to the satellite network device 200, where the first data packet includes the first sequence number field.

[001218] The terminal 100 may update the value of the first sequence number after sending the first data packet to the satellite network device 200. An updated value of the first sequence number is different from the value that is of the first sequence number and that exists before the update. It may be understood that, when the updated value of the first sequence number is less than the value that is of the first sequence number and that exists before the update, the terminal 100 may update a value of the first hyper frame number. The first information is updated as the first sequence number is updated.

[001219] Specifically, the terminal 100 may update a value of the first information by updating the first sequence number and the first hyper frame number. After the value of the first sequence number is updated from the initial value to a maximum value, the terminal 100 updates the value

of the first sequence number to the initial value again. After determining that the updated value of the first sequence number is less than or equal to the value that is of the first sequence number and that exists before the update, the terminal 100 may update the value of the first hyper frame number, that is, add a preset value to the value of the first hyper frame number. Likewise, after the value of the first hyper frame number is updated from the initial value to a maximum value, the terminal 100 updates the value of the first hyper frame number to the initial value again, that is, updates the value of the first information to an initial value.

[001220] For example, a length of the first information is 5 bits, the first hyper frame number may be 4 bits in a header of the first information, and the first sequence number may be 1 bit behind the first hyper frame number in the first information. The initial value of the first information may be "00000", that is, the initial value of the first hyper frame number is "0000", and the initial value of the first sequence number is "0". After the terminal 100 sends, to the satellite network device 200, a first data packet generated based on a first sequence number whose value is "0", the terminal 100 may update the value of the first sequence number to "1", that is, update the value of the first information to "00001".

[001221] After the terminal 100 sends, to the satellite network device 200, a first data packet generated based on a first sequence number whose value is "1", the terminal 100 may update the value of the first sequence number to "0". The terminal 100 determines that the updated value "0" of the first sequence number is less than the value "1" existing before the update, and updates the value of the first hyper frame number to "0001", that is, updates the value of the first information to "00010". After sending, to the satellite network device 200, a first data packet generated based on a first sequence number whose value is "0", the terminal 100 updates the value of the first sequence number to "1". The rest can be deduced from this.

[001222] Likewise, when a length of the first information is 5 bits, the first hyper frame number is 3 bits in a header of the first information, and a length of the first sequence number is 2 bits behind the first hyper frame number in the first information, the initial value of the first information may be "00000", that is, the initial value of the first hyper frame number is "000", and the initial value of the first sequence number is "00". After the terminal 100 sends, to the satellite network device 200, a first data packet generated based on a first sequence number whose value is "00", the terminal 100 may update the value of the first sequence number to "01", that is, update the value of the first information to "00001".

[001223] After the terminal 100 sends, to the satellite network device 200, a first data packet generated based on a first sequence number whose value is "01", the terminal 100 may update the value of the first sequence number to "10", that is, update the value of the first information to "00010".

[001224] After the terminal 100 sends, to the satellite network device 200, a first data packet generated based on a first sequence number whose value is "10", the terminal 100 may update the value of the first sequence number to "11", that is, update the value of the first information to "00011".

[001225] After the terminal 100 sends, to the satellite network device 200, a first data packet generated based on a first sequence number whose value is "11", the terminal 100 may update the value of the first sequence number to "00". The terminal 100 determines that the updated value "00" of the first sequence number is less than the value "11" existing before the update, and updates the value of the first hyper frame number to "001", that is, updates the value of the first information to "00100".

[001226] In conclusion, the terminal 100 may update the first information by updating the first sequence number.

[001227] In a possible implementation, after sending the first data packet to the receiving device, the terminal 100 may display sending prompt information. The sending prompt information may be used to prompt a user that the terminal 100 has sent the first data packet to the satellite network device 200.

[001228] S3206: The satellite network device 200 may determine the second information based on the first sequence number field and the second hyper frame number.

[001229] The satellite network device 200 stores the second sequence number. A value of the second sequence number is a value of a first sequence number field of a previous first data packet received by the satellite network device 200.

[001230] In some embodiments, when the satellite network device 200 does not receive a first data packet of the terminal 100, the initial value of the second sequence number may be a null value. The satellite network device 200 may be preset to determine that the initial value of the second sequence number is less than any value. Optionally, the initial value of the second sequence number pre-stored in the satellite network device 200 is less than the initial value of the first sequence number of the terminal 100.

[001231] The satellite network device 200 may determine whether the value of the first sequence number field is greater than the value of the second sequence number. When the satellite network device 200 determines that the value of the first sequence number field is greater than the value of the second sequence number, the satellite network device 200 may concatenate a value of the second hyper frame number and the value of the first sequence number field, to obtain a value of the second information.

[001232] When the satellite network device 200 determines that the value of the first sequence number field is less than or equal to the value of the second sequence number, the satellite network

device 200 may update a value of the second hyper frame number, that is, add a preset value to the value of the second hyper frame number. The satellite network device 200 may concatenate an updated value of the second hyper frame number and the value of the first sequence number field, to obtain a value of the second information.

[001233] After generating the second information, the satellite network device 200 may adjust the value of the second sequence number based on the value of the first sequence number field. An adjusted value of the second sequence number is equal to the value of the first sequence number.

[001234] For example, when a length of the second information of the satellite network device 200 is 5 bits, the second hyper frame number is 4 bits in a header of the second information, and a length of the second sequence number is 1 bit behind the second hyper frame number in the second information, the initial value of the second hyper frame number of the satellite network device 200 is "0000". After receiving the first data packet whose first sequence number field is "0", the satellite network device 200 may determine that the value of the second information is "00000", and the value of the second sequence number is "0".

[001235] After receiving the first data packet whose first sequence number field is "1", the satellite network device 200 may determine, based on the value of the second sequence number and the value of the first sequence number field, that the value of the second information is "00001", and the value of the second sequence number is "1".

[001236] After receiving the first data packet whose first sequence number field is "0", the satellite network device 200 may determine, based on the value of the second sequence number and the value of the first sequence number field, that the value of the second hyper frame number is "0001", and then determine that the value of the second information is "00010", and the value of the second sequence number is "0". The rest can be deduced from this.

[001237] It should be noted that, if the satellite network device 200 does not receive the first data packet whose first sequence number is "1", after the satellite network device 200 receives the second data packet whose first sequence number is "0", because the value of the second sequence number is equal to the value of the first sequence number field, the satellite network device 200 can accordingly determine that the value of the second hyper frame number is "0001", and can successfully receive the second data packet whose first sequence number is "0". In this way, even if a data packet sent by the terminal 100 is lost in a sending process, the satellite network device 200 can successfully obtain the value of the second information corresponding to the first information.

[001238] In a possible implementation, the first hyper frame number pre-stored in the terminal 100 is greater than the second hyper frame number pre-stored in the satellite network device 200 by a preset value, and an initial value of the second sequence number pre-stored in the satellite

network device 200 is greater than a maximum value of the first sequence number of the terminal 100. After the terminal 100 sends, to the satellite network device 200, the first data packet including the first sequence number field, the satellite network device 200 may add the preset value to a value of the second hyper frame number based on a fact that a value of the first sequence number field is the same asa value of the second sequence number, so that the value of the second hyper frame number is the same as a value of the first hyper frame number of the terminal 100. Then, the satellite network device 200 may adjust the value of the second sequence number to be the same as the value of the first sequence number field.

[001239] S3207: The satellite network device 200 may generate a second authentication code based on the specified key, the original data, and the second information.

[001240] S3208: The satellite network device 200 determines whether the first authentication code is the same as the second authentication code.

[001241] The satellite network device 200 may determine a receiving status of the first data packet by determining, through comparison, whether the first authentication code is the same as the second authentication code. When the first authentication code is the same as the second authentication code, the satellite network device 200 may perform step S3209 and step S3210.

[001242] When the first authentication code is different from the second authentication code, the satellite network device 200 may perform step S3212.

[001243] S3209: The satellite network device 200 sends the original data to the cellular network device 400.

[001244] S3210: The satellite network device 200 sends a success application receipt to the terminal 100.

[001245] S3211: The terminal 100 displays success prompt information.

[001246] The terminal 100 displays the success prompt information. The success prompt information prompts the user that the first data packet is successfully sent.

[001247] S3212: The satellite network device 200 sends a failure application receipt to the terminal 100.

[001248] Optionally, after receiving the failure application receipt, the terminal 100 may further perform step S3213.

[001249] S3213: The terminal 100 displays failure prompt information.

[001250] The terminal 100 displays the failure prompt information. The failure prompt information prompts the user that the first data packet fails to be sent.

[001251] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 12. Details are not described herein again.

[001252] The following describes an outbound procedure of another transmission method

according to an embodiment of this application.

[001253] In a possible implementation, in an outbound process, a satellite network device 200 may generate a fourth authentication code based on sixth information and original data. The sixth information is sixth context information, and may indicate a sequence number of a third data packet. The satellite network device 200 may obtain, based on a fourth sequence number field, the fourth authentication code, and the original data, the third data packet including the fourth sequence number field (also referred to as sixth indication information). The satellite network device 200 may send the third data packet to a terminal 100. After receiving the third data packet, the terminal 100 may determine fifth information based on the fourth sequence number field, and generate a third authentication code based on the fifth information and the third data packet. The fifth information is fifth context information, and indicates a sequence number of the third data packet. The terminal 100 may determine a receiving status of the third data packet based on the third authentication code. In this way, a problem that the terminal 100 repeatedly receives a same data packet does not occur, and the terminal 100 and the satellite network device 200 can further continue to transmit a next data packet after an application receipt/a data packet is lost.

[001254] FIG. 33 is a schematic diagram of an outbound transmission procedure according to an embodiment of this application.

[001255] S3301: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about fifth information and sixth information.

[001256] The terminal 100 and the satellite network device 200 may obtain an initial value of the sixth information and an initial value of the fifth information through negotiation by using the cellular network device 400. The satellite network device 200 stores a fourth hyper frame number and a fourth sequence number in the sixth information. The terminal 100 stores a third hyper frame number and a third sequence number in the fifth information. An initial value of the third hyper frame number in the fifth information is the same as an initial value of the fourth hyper frame number in the sixth information. An initial value of the third sequence number in the fifth information is less than an initial value of the fourth sequence number in the sixth information.

[001257] S3302: The satellite network device 200 receives original data sent by the cellular network device 400.

[001258] S3303: The satellite network device 200 receives a service request sent by the terminal 100.

[001259] S3304: The satellite network device 200 generates a fourth authentication code based on the original data and the sixth information.

[001260] The satellite network device 200 may generate the fourth authentication code based on the sixth information and the original data.

[001261] S3305: The satellite network device 200 obtains a third data packet based on the fourth sequence number, the original data, and the fourth authentication code.

[001262] The sixth information of the satellite network device 200 includes the fourth sequence number and the fourth hyper frame number. The satellite network device 200 may generate a fourth sequence number field (also referred to as sixth indication information) based on the fourth sequence number. A value of the fourth sequence number field is the same as a value of the fourth sequence number. The satellite network device 200 may concatenate the fourth sequence number field, the fourth authentication code, and the original data, to obtain the third data packet.

[001263] S3306: The satellite network device 200 sends the third data packet to the terminal 100, where the third data packet includes the fourth sequence number field.

[001264] The satellite network device 200 may update the value of the fourth sequence number after sending the third data packet to the terminal 100. An updated value of the fourth sequence number is different from the value that is of the fourth sequence number and that exists before the update. It may be understood that, when the updated value of the fourth sequence number is less than the value that is of the fourth sequence number and that exists before the update, the satellite network device 200 may update a value of the fourth hyper frame number. The sixth information is updated as the fourth sequence number is updated.

[001265] Specifically, the satellite network device 200 may update a value of the sixth information by updating the fourth sequence number. After the value of the fourth sequence number is updated from the initial value to a maximum value, the satellite network device 200 updates the value of the fourth sequence number to the initial value again. After determining that the updated value of the fourth sequence number is less than or equal to the value that is of the fourth sequence number and that exists before the update, the satellite network device 200 may update the value of the fourth hyper frame number, that is, add a preset value to the value of the fourth hyper frame number. Likewise, after the value of the fourth hyper frame number is updated from the initial value to a maximum value, the satellite network device 200 updates the value of the fourth hyper frame number to the initial value again, that is, updates the value of the sixth information to the initial value.

[001266] S3307: The terminal 100 determines the fifth information based on the fourth sequence number field and the third hyper frame number.

[001267] The terminal 100 stores the third sequence number. A value of the third sequence number is a value of a fourth sequence number field of a previous third data packet received by the terminal 100.

[001268] In some embodiments, when the terminal 100 does not receive a third data packet of the satellite network device 200, the initial value of the third sequence number may be a null value.

The terminal 100 may be preset to determine that the initial value of the third sequence number is less than any value. Optionally, the initial value of the third sequence number pre-stored in the terminal 100 is less than the initial value of the fourth sequence number of the satellite network device 200.

[001269] The terminal 100 may determine whether the value of the fourth sequence number field is greater than the value of the third sequence number. When the terminal 100 determines that the value of the fourth sequence number field is greater than the value of the third sequence number, the terminal 100 may concatenate a value of the third hyper frame number and the value of the fourth sequence number field, to obtain a value of the fifth information.

[001270] When the terminal 100 determines that the value of the fourth sequence number field is less than or equal to the value of the third sequence number, the terminal 100 may update a value of the third hyper frame number, that is, add a preset value to the value of the third hyper frame number. The terminal 100 may concatenate an updated value of the third hyper frame number and the value of the fourth sequence number field, to obtain a value of the fifth information.

[001271] After generating the fifth information, the terminal 100 may adjust the value of the third sequence number based on the value of the fourth sequence number field. An adjusted value of the third sequence number is equal to the value of the fourth sequence number.

[001272] In a possible implementation, the fourth hyper frame number pre-stored in the satellite network device 200 is greater than the third hyper frame number pre-stored in the terminal 100 by a preset value, and an initial value of the third sequence number pre-stored in the terminal 100 is greater than a maximum value of the fourth sequence number pre-stored in the satellite network device 200. After the satellite network device 200 sends, to the terminal 100, the third data packet including the fourth sequence number field, the terminal 100 may add the preset value to a value of the third hyper frame number based on a fact that a value of the fourth sequence number field is the same as a value of the third sequence number, so that the value of the third hyper frame number is the same as a value of the fourth hyper frame number of the satellite network device 200. Then, the terminal 100 may update the value of the third sequence number to the value of the fourth sequence number field.

[001273] S3308: The terminal 100 obtains a third authentication code based on the third data packet and the fifth information.

[001274] S3309: The terminal 100 determines whether the third authentication code is the same as the fourth authentication code.

[001275] The terminal 100 may determine a receiving status of the third data packet by determining, through comparison, whether the third authentication code is the same as the fourth authentication code. When the third authentication code is the same as the fourth authentication

code, the terminal 100 may perform step S3310 and step S3311.

[001276] When the third authentication code is different from the fourth authentication code, the terminal 100 may perform step S3312.

[001277] S3310: The terminal 100 displays receiving prompt information.

[001278] S3311: The terminal 100 sends a success application receipt to the satellite network device 200.

[001279] S3312: The terminal 100 sends a failure application receipt to the satellite network device 200.

[001280] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 13. Details are not described herein again.

[001281] The following describes a procedure in which a sending device and a receiving device transmit a data packet based on a sequence number. Details are shown in FIG. 34.

[001282] S3401: A sending device obtains a data packet 1 based on context information A (including a sequence number A) and original data, where a value of the context information A is X||y1, || is a concatenation symbol, and a value of the sequence number A is y1.

[001283] The sending device may obtain a sequence number field A based on the sequence number A in the context information A. The sending device may generate an authentication code A based on the context information A and the original data. The sending device may obtain the data packet 1 based on the sequence number field A, the authentication code A, and the original data. The context information A includes the sequence number A and a hyper frame number A. A value of the hyper frame number A is X, and the value of the sequence number A is y1. The context information A is a data segment obtained by concatenating the hyper frame number A and the sequence number A together.

[001284] S3402: The sending device sends the data packet 1 to a receiving device, where the data packet 1 includes the sequence number field A and the authentication code A.

[001285] After sending the data packet 1 to the receiving device, the sending device may update the value of the sequence number A to y2. y2 is greater than y1. That is, the sending device updates the value of the context information A to X||y2.

[001286] It should be noted that, when the value of the sequence number A includes only y1 and y2, the sending device may add a preset value to the value of the hyper frame number A when updating the value of the sequence number A to y1 again after updating the value of the sequence number A to y2.

[001287] S3403: After determining a value of a hyper frame number B based on the sequence number field A, the receiving device generates an authentication code B based on the hyper frame number B, the sequence number field A, and the data packet 1, where the value of the hyper frame

number B is X.

[001288] The receiving device may determine the value of the hyper frame number B based on a value of the sequence number field A. Specifically, when determining that the value of the sequence number field A is less than or equal to a value of a sequence number B, the receiving device may add a preset value to the value of the hyper frame number B.

[001289] When the receiving device receives the 1st data packet of the sending device, the value of the sequence number B is an initial value, and the initial value of the sequence number B is less than an initial value of the sequence number A. After generating context information B, the receiving device may update the value of the sequence number B to the value of the sequence number A. When the receiving device receives the 2nd data packet sent by the sending device, the value of the sequence number B is the same as a value of a sequence number field A of the 1st data packet.

[001290] The receiving device may concatenate the value of the hyper frame number B and the value of the sequence number field A, to obtain context information B that is X||y1. After obtaining the context information B, the receiving device may further update the value of the sequence number B to the value of the sequence number field A. For specific descriptions, refer to the foregoing embodiments. Details are not described herein again.

[001291] The receiving device may generate the authentication code B based on the context information B and the original data in the data packet 1. Herein, the value of the hyper frame number B is X, and an updated value of the sequence number B is y1. The value that is of the sequence number B and that exists before the update is smaller than y1.

[001292] S3404: The receiving device determines that the authentication code A is the same as the authentication code B, and generates a success application receipt.

[001293] S3405: The receiving device sends the success application receipt to the sending device.

[001294] S3406: The sending device obtains a data packet 2 based on the context information A (including the sequence number A) and original data, where the value of the context information A is X||y2, and the value of the sequence number A is y2.

[001295] In this way, the sending device and the receiving device can resolve, based on context information indicating a sequence number, a problem of repeatedly receiving a same data packet.

[001296] The following describes a case in which data may be lost in a sending process in embodiments of this application.

[001297] A data packet/a success application receipt may be lost in a transmission process of a sending device and a receiving device. Details are shown in FIG. 35A and FIG. 35B.

[001298] S3501: A sending device obtains a data packet 1 based on context information A (including a sequence number A), where a value of the context information A is X||y1, || is a

concatenation symbol, and a value of the sequence number A is y1.

[001299] S3502: The sending device fails to send the data packet 1 to a receiving device, where the data packet 1 includes a sequence number field A and an authentication code A.

[001300] The data packet 1 is lost in a transmission process, and therefore the receiving device does not receive the data packet 1.

[001301] After sending the data packet 1 to the receiving device, the sending device may update the value of the sequence number A to y2. y2 is greater than y1. That is, the sending device updates the value of the context information A to X||y2.

[001302] S3503: The sending device obtains a data packet 2 based on the context information A (including the sequence number A), where the value of the context information A is X||y2, and the value of the sequence number A is y2.

[001303] S3504: The sending device sends the data packet 2 to the receiving device, where the data packet 2 includes a sequence number field A and an authentication code A.

[001304] After sending the data packet 2 to the receiving device, the sending device may update the value of the sequence number A to y1. Because the value of the sequence number A is updated to y1 again, the sending device may update a value of a hyper frame number A to X+i. That is, the sending device updates the value of the context information A to (X+i)||y1.

[001305] S3505: After determining a value of a hyper frame number B based on the sequence number field A, the receiving device generates an authentication code B based on the hyper frame number B, the sequence number field A, and the data packet 2, where the value of the hyper frame number B is X.

[001306] The receiving device may determine, based on a value of the sequence number field A, that the value of the hyper frame number B is X. The receiving device may concatenate the value of the hyper frame number B and the value of the sequence number field A, to obtain context information B that is X||y2. The receiving device may generate the authentication code B based on the context information B and the data packet 2.

[001307] After obtaining the context information B, the receiving device may further update a value of a sequence number B to the value of the sequence number field A. For specific descriptions, refer to the foregoing embodiments. Details are not described herein again. Herein, an updated value of the sequence number B is y2. The value that is of the sequence number B and that exists before the update is smaller than y2.

[001308] S3506: The receiving device determines that the authentication code A is the same as the authentication code B, and generates a success application receipt.

[001309] S3507: The receiving device fails to send the success application receipt to the sending device.

[001310] In a sending process, a data packet may be lost and an application receipt may be lost. When the sending device sends a data packet to the receiving device, and the receiving device does not receive the data packet of the sending device, transmission of a next data packet between the sending device and the receiving device is not affected.

[001311] S3508: The sending device obtains a data packet 3 based on the context information A (including the sequence number A) and original data, where the value of the context information A is (X+i)||y1, and the value of the sequence number A is y1.

[001312] S3509: The sending device fails to send the data packet 3 to the receiving device, where the data packet 3 includes a sequence number field A and an authentication code A.

[001313] The data packet 3 is lost in a transmission process, and therefore the receiving device does not receive the data packet 3.

[001314] After sending the data packet 3 to the receiving device, the sending device may update the value of the sequence number A to y2. That is, the sending device updates the value of the context information A to (X+i)||y2.

[001315] S3510: The sending device obtains a data packet 4 based on the context information A (including the sequence number A) and original data, where the value of the context information A is (X+i)||y2, and the value of the sequence number A is y2.

[001316] S3511: The sending device fails to send the data packet 4 to the receiving device, where the data packet 4 includes a sequence number field A and an authentication code A.

[001317] The data packet 4 is lost in a transmission process, and therefore the receiving device does not receive the data packet 4.

[001318] After sending the data packet 4 to the receiving device, the sending device may update the value of the sequence number A to y1. Because the value of the sequence number A is updated to y1 again, the sending device may update the value of the hyper frame number A to X+2i. That is, the sending device updates the value of the context information A to (X+2i)||y1.

[001319] S3512: The sending device obtains a data packet 5 based on the context information A (including the sequence number A) and original data, where the value of the context information A is (X+2i)||y1, and the value of the sequence number A is y1.

[001320] S3513: The sending device sends the data packet 5 to the receiving device, where the data packet 5 includes a sequence number field A and an authentication code A.

[001321] After sending the data packet 5 to the receiving device, the sending device may update the value of the sequence number A to y2. That is, the sending device updates the value of the context information A to (X+2i)||y2.

[001322] S3514: After determining the value of the hyper frame number B based on the sequence number field A, the receiving device generates an authentication code B based on the hyper frame

number B, the sequence number field A, and the data packet 5, where the value of the hyper frame number B is (X+i).

[001323] A current value of the hyper frame number of the receiving device is X, and a current value of the sequence number B is y2. The receiving device determines that the value of the sequence number field A is y1. y1 is less than y2. The receiving device updates the value of the hyper frame number B to X+i, and obtain, based on the value of the hyper frame number B and the value of the sequence number field A, the value of the context information B: (X+i)||y1. The receiving device generates an authentication code B based on the context information B.

[001324] When the receiving device does not receive data packets of the sending device for a plurality of consecutive times, because the hyper frame number B may be inconsistent with the hyper frame number A, the receiving device cannot successfully receive a data packet of the sending device.

[001325] In a possible implementation, when determining that the authentication code A is different from the authentication code B, the receiving device may adjust the value of the hyper frame number B and the value of the sequence number B to initial values, and sends a failure application receipt to the sending device. The sending device may adjust the value of the context information A to an initial value based on the failure application receipt. In this way, the sending device and the receiving device can transmit a data packet based on reset context information.

[001326] S3515: The receiving device determines that the authentication code A is different from the authentication code B, and resets the value of the hyper frame number B to X.

[001327] The value of the context information B of the receiving device is (X+i)||y1 and is different from the context information A "(X+2i)||y1" used by the sending device to generate the data packet 5. Therefore, the authentication code A is different from the authentication code B. The receiving device fails to receive the data packet 5, and the receiving device may reset the value of the hyper frame number B to an initial value, for example, the initial value X. The receiving device may further reset the value of the sequence number B to an initial value.

[001328] S3516: The receiving device sends a failure application receipt to the sending device.

[001329] After determining that the authentication code A is different from the authentication code B, the receiving device may generate the failure application receipt. The failure application receipt indicates that the receiving device fails to receive the data packet 5. The receiving device sends the failure application receipt to the sending device.

[001330] S3517: The sending device resets the value of the context information A to X||y1.

[001331] The sending device may determine, based on the failure application receipt, that the value of the context information A is not synchronized with the value of the context information B. The sending device may reset the value of the context information A to the initial value, for

example, the initial value X||y1.

[001332] For specific descriptions of the foregoing steps, refer to the embodiment shown in FIG. 34. Details are not described herein again.

[001333] This application is not limited to the foregoing embodiments, and further provides the following embodiments. It should be noted that the following embodiments may be used in mutual combination with any one or more of the foregoing embodiments.

[001334] In a possible implementation, a sending device may obtain, based on a retransmission indication field, information A, and original data, a data packet including an authentication code A and the retransmission indication field. The information A is sending time information or context information A. The retransmission indication field indicates that the data packet is a retransmitted data packet or a newly transmitted data packet. A receiving device may obtain an authentication code B based on information B and the data packet. The information B is receiving time information or context information B. When the authentication code A is different from the authentication code B, when determining, based on the retransmission indication field, that the data packet is a newly transmitted data packet, the receiving device may send a failure application receipt to the sending device. When determining, based on the retransmission indication field, that the data packet is a retransmitted data packet, the receiving device may generate an authentication code C. When the authentication code A is the same as the authentication code C, the receiving device may determine that the data packet is a retransmitted data packet corresponding to a data packet latest successfully received by the receiving device. The receiving device sends a success application receipt to the sending device.

[001335] In this way, when determining that the authentication code B is different from the authentication code A of the newly transmitted data packet, the receiving device determines that the receiving device fails to receive the newly transmitted data packet, and directly sends the failure application receipt. When the receiving device determines that the authentication code C is the same as the authentication code A of the retransmitted data packet, the receiving device may determine that the data packet is the retransmitted data packet corresponding to the latest successfully received data packet, that is, the receiving device may determine that the sending device fails to receive a success application receipt of the latest successfully received data packet, and the receiving device may send the success application receipt to the sending device again. The sending device may determine, based on the success application receipt, that original data in the retransmitted data packet is successfully sent, and no longer perform a retransmission operation, thereby saving a transmission resource of a satellite network.

[001336] The following describes an inbound procedure of another transmission method according to an embodiment of this application.

[001337] In a possible implementation, in an inbound process, a terminal 100 may generate a first authentication code based on first information, a specified key, and original data. The first information is sending time information or first context information. The terminal 100 may obtain a first data packet based on a first retransmission indication field (also referred to as third indication information), the first authentication code, the specified key, and the original data. The terminal 100 may send the first data packet to a satellite network device 200 in a first transmission system. After receiving the first data packet, the satellite network device 200 may generate a second authentication code based on second information, the specified key, and the first data packet. The second information is receiving time information or second context information. When the first authentication code is different from the second authentication code, when determining, based on the first retransmission indication field, that the first data packet is a retransmitted data packet, the satellite network device 200 may generate a temporary authentication code, and when determining that the first authentication code is the same as the temporary authentication code, send a success application receipt to the terminal 100. In this way, the satellite network device 200 can notify, based on the success application receipt, the terminal 100 that the satellite network device 200 has successfully received the original data in the retransmitted data packet, and the terminal 100 does not need to retransmit the data packet again.

[001338] FIG. 36A and FIG. 36B are a schematic diagram of an inbound transmission procedure according to an embodiment of this application.

[001339] S3601: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about a key, first information, and second information.

[001340] For descriptions of negotiating about the key, the first information, and a second hyper frame number by the terminal 100, the satellite network device 200, and the cellular network device 400, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again. After negotiating about the key, both the terminal 100 and the satellite network device 200 store the specified key. The terminal 100 stores the first information. The satellite network device 200 stores the second information. An initial value of the first information is the same as an initial value of the second information.

[001341] S3602: The terminal 100 obtains original data.

[001342] S3603: The terminal 100 generates a first authentication code based on the specified key, the original data, and the first information.

[001343] The terminal 100 may obtain the first authentication code through calculation based on the stored first information, the specified key, and the original data by using a specified authentication algorithm (for example, an SM3 hash algorithm).

[001344] S3604: The terminal 100 may obtain a first data packet based on a first retransmission

indication field, the first authentication code, and the original data.

[001345] The terminal 100 may concatenate the first retransmission indication field, the first authentication code, and the original data, to obtain the first data packet.

[001346] For example, when a length of the first retransmission indication field is 1 bit, if a value of the first retransmission indication field is "0", the first retransmission indication field may indicate that the first data packet is a newly transmitted data packet. If a value of the first retransmission indication field is "1", the first retransmission indication field may indicate that the first data packet is a retransmitted data packet.

[001347] In a possible implementation, when receiving input of a satellite message retransmitted by a user, the terminal 100 may generate original data and a first retransmission indication field based on the satellite message. The first retransmission indication field indicates that a data packet generated based on the original data in the satellite message is a retransmitted data packet.

[001348] In a possible implementation, the terminal 100 may detect whether current original data is the same as original data in a previous data packet. When determining that the current original data is the same as the original data in the previous data packet, the terminal 100 generates a first retransmission indication field indicating that a data packet including the current original data is a retransmitted data packet. When determining that the current original data is different from the original data in the previous data packet, the terminal 100 generates a first retransmission indication field indicating that a data packet including the current original data is a newly transmitted data packet.

[001349] In a possible implementation, the terminal 100 may further encrypt, by using the specified key, the first authentication code and the original data that are concatenated together, to obtain the first data packet. Optionally, the terminal 100 may encrypt, by using the specified key, the first retransmission indication field, the first authentication code, and the original data that are concatenated together, to obtain the first data packet.

[001350] S3605: The terminal 100 sends the first data packet to the satellite network device 200, where the first data packet includes the first retransmission indication field.

[001351] In a possible implementation, after sending the first data packet to the receiving device, the terminal 100 may display sending prompt information. The sending prompt information may be used to prompt the user that the terminal 100 has sent the first data packet to the satellite network device 200.

[001352] S3606: The satellite network device 200 may generate a second authentication code based on the specified key, the first data packet, and second information.

[001353] S3607: The satellite network device 200 determines whether the first authentication code is the same as the second authentication code.

[001354] The satellite network device 200 may determine a receiving status of the first data packet by determining, through comparison, whether the first authentication code is the same as the second authentication code. When the first authentication code is the same as the second authentication code, the satellite network device 200 may perform step S3608 and step S3609.

[001355] When the first authentication code is different from the second authentication code, the satellite network device 200 may perform step S3611.

[001356] S3608: The satellite network device 200 sends the original data to the cellular network device 400.

[001357] S3609: The satellite network device 200 sends a success application receipt to the terminal 100.

[001358] Optionally, after receiving the success application receipt, the terminal 100 may further perform step S3610.

[001359] S3610: The terminal 100 displays success prompt information.

[001360] After receiving the success application receipt sent by the satellite network device 200, the terminal 100 may further display the success prompt information. The success prompt information prompts the user that the first data packet is successfully sent.

[001361] S3611: The satellite network device 200 determines, based on the first retransmission indication field, whether the first data packet is a retransmitted data packet.

[001362] When determining, based on the first retransmission indication field, that the first data packet is a newly transmitted data packet, the satellite network device 200 may perform step S3612.

[001363] When determining, based on the first retransmission indication field, that the first data packet is a retransmitted data packet, the satellite network device 200 may perform step S3614 to step S3616.

[001364] S3612: The satellite network device 200 sends a failure application receipt to the terminal 100.

[001365] Optionally, after receiving the failure application receipt, the terminal 100 may further perform step S3613.

[001366] S3613: The terminal 100 displays failure prompt information.

[001367] The terminal 100 displays the failure prompt information. The failure prompt information prompts the user that the first data packet fails to be sent.

[001368] S3614: The satellite network device 200 obtains temporary information based on the second information.

[001369] The satellite network device 200 may subtract a preset value from a value of the second information, to obtain the temporary information.

[001370] S3615: The satellite network device 200 may generate a temporary authentication code

based on the specified key, the first data packet, and the temporary information.

[001371] S3616: The satellite network device 200 may determine whether the first authentication code is the same as the temporary authentication code.

[001372] When the first authentication code is the same as the temporary authentication code, the satellite network device 200 may perform step S3617.

[001373] When the first authentication code is different from the temporary authentication code, the satellite network device 200 may perform step S3619.

[001374] S3617: The satellite network device 200 sends a success application receipt to the terminal 100.

[001375] When determining that the first authentication code is the same as the temporary authentication code, the satellite network device 200 may determine that the satellite network device 200 has received a newly transmitted data packet corresponding to the retransmitted data packet. The satellite network device 200 may determine that the terminal 100 does not receive a success application receipt indicating that the receiving device successfully receives the newly transmitted data packet corresponding to the retransmitted data packet, and the satellite network device 200 may send the success application receipt to the terminal 100. The success application receipt may indicate that the satellite network device 200 successfully receives the original data in the retransmitted data packet.

[001376] Optionally, after receiving the success application receipt, the terminal 100 may further perform step S3618.

[001377] S3618: The terminal 100 displays success prompt information.

[001378] After receiving the success application receipt sent by the satellite network device 200, the terminal 100 may further display the success prompt information. The success prompt information prompts the user that the first data packet is successfully sent.

[001379] S3619: The satellite network device 200 sends a failure application receipt to the terminal 100.

[001380] Optionally, after receiving the failure application receipt, the terminal 100 may further perform step S3620.

[001381] S3620: The terminal 100 displays failure prompt information.

[001382] The terminal 100 displays the failure prompt information. The failure prompt information prompts the user that the first data packet fails to be sent.

[001383] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 12. Details are not described herein again.

[001384] The following describes an outbound procedure of another transmission method according to an embodiment of this application.

[001385] In a possible implementation, in an outbound process, a satellite network device 200 may generate a fourth authentication code based on sixth information and original data. The sixth information is sending time information or sixth context information. The satellite network device 200 may obtain a third data packet based on a second retransmission indication field (also referred to as fourth indication information), a fourth authentication code, and original data. The satellite network device 200 may send the third data packet to a terminal 100 in a first transmission system. After receiving the third data packet, the terminal 100 may generate a third authentication code based on fifth information and the third data packet. The fifth information is receiving time information or fifth context information. When the third authentication code is different from the fourth authentication code, when determining, based on the second retransmission indication field, that the third data packet is a retransmitted data packet, the terminal 100 may generate a temporary authentication code, and when determining that the fourth authentication code is the same as the temporary authentication code, send a success application receipt to the satellite network device 200. In this way, the terminal 100 may notify, based on the success application receipt, the satellite network device 200 that the terminal 100 has successfully received the original data in the retransmitted data packet, and the satellite network device 200 does not need to retransmit the data packet again.

[001386] FIG. 37A and FIG. 37B are a schematic diagram of an outbound transmission procedure according to an embodiment of this application.

[001387] S3701: A terminal 100, a satellite network device 200, and a cellular network device 400 negotiate about fifth information and sixth information.

[001388] For a process in which the terminal 100 and the satellite network device 200 obtain the sixth information and the fifth information through negotiation, refer to the foregoing embodiment shown in FIG. 11A and FIG. 11B. Details are not described herein again. The satellite network device 200 stores the sixth information. The terminal 100 stores the fifth information. An initial value of the fifth information is the same as an initial value of the sixth information.

[001389] S3702: The satellite network device 200 receives original data sent by the cellular network device 400.

[001390] S3703: The satellite network device 200 receives a service request sent by the terminal 100.

[001391] S3704: The satellite network device 200 generates a fourth authentication code based on the original data and the sixth information.

[001392] The satellite network device 200 may generate the fourth authentication code based on the stored sixth information and the original data.

[001393] S3705: The satellite network device 200 obtains a third data packet based on a second

retransmission indication field, the original data, and the fourth authentication code.

[001394] The satellite network device 200 may concatenate the second retransmission indication field, the fourth authentication code, and the original data, to obtain the third data packet.

[001395] For example, when a length of the second retransmission indication field is 1 bit, if a value of the second retransmission indication field is "0", the second retransmission indication field may indicate that the third data packet is a newly transmitted data packet. If a value of the second retransmission indication field is "1", the second retransmission indication field may indicate that the third data packet is a retransmitted data packet.

[001396] In a possible implementation, the satellite network device 200 may detect whether current original data is the same as original data in a previous data packet. When determining that the current original data is the same as the original data in the previous data packet, the satellite network device 200 generates a second retransmission indication field indicating that a data packet including the current original data is a retransmitted data packet. When determining that the current original data is different from the original data in the previous data packet, the satellite network device 200 generates a first retransmission indication field indicating that a data packet including the current original data is a newly transmitted data packet.

[001397] S3706: The satellite network device 200 sends the third data packet to the terminal 100, where the third data packet includes the second retransmission indication field.

[001398] S3707: The terminal 100 obtains a third authentication code based on the third data packet and the fifth information.

[001399] S3708: The terminal 100 determines whether the third authentication code is the same as the fourth authentication code.

[001400] The terminal 100 may determine a receiving status of the third data packet by determining, through comparison, whether the third authentication code is the same as the fourth authentication code. When the third authentication code is the same as the fourth authentication code, the terminal 100 may perform step S3709 and step S3710.

[001401] When the third authentication code is different from the fourth authentication code, the terminal 100 may perform step S3711.

[001402] S3709: The terminal 100 displays receiving prompt information.

[001403] S3710: The terminal 100 sends a success application receipt to the satellite network device 200.

[001404] S3711: The terminal 100 determines, based on the second retransmission indication field, whether the third data packet is a retransmitted data packet.

[001405] When determining, based on the second retransmission indication field, that the third data packet is a newly transmitted data packet, the terminal 100 may perform step S3712.

[001406] When determining, based on the second retransmission indication field, that the third data packet is a retransmitted data packet, the terminal 100 may perform step S3713 to step S3715.

[001407] S3712: The terminal 100 sends a failure application receipt to the satellite network device 200.

[001408] S3713: The terminal 100 obtains temporary information based on the fifth information.

[001409] The terminal 100 may subtract a preset value from a value of the fifth information, to obtain the temporary information.

[001410] S3714: The terminal 100 may generate a temporary authentication code based on the specified key, the third data packet, and the temporary information.

[001411] S3715: The terminal 100 may determine whether the fourth authentication code is the same as the temporary authentication code.

[001412] When the fourth authentication code is the same as the temporary authentication code, the terminal 100 may perform step S3716.

[001413] When the fourth authentication code is different from the temporary authentication code, the terminal 100 may perform step S3717.

[001414] S3716: The terminal 100 sends a success application receipt to the satellite network device 200.

[001415] When determining that the fourth authentication code is the same as the temporary authentication code, the terminal 100 may determine that the terminal 100 has received a newly transmitted data packet corresponding to the retransmitted data packet. The terminal 100 may determine that the satellite network device 200 does not receive a success application receipt indicating that the receiving device successfully receives the newly transmitted data packet corresponding to the retransmitted data packet, and the terminal 100 may send the success application receipt to the satellite network device 200. The success application receipt may indicate that the terminal 100 successfully receives the original data in the retransmitted data packet.

[001416] S3717: The terminal 100 sends a failure application receipt to the satellite network device 200.

[001417] For specific descriptions of the foregoing steps, refer to the foregoing embodiment shown in FIG. 13. Details are not described herein again.

[001418] The following describes, with reference to a method in which context information indicates information about a quantity of data packets, a transmission procedure of a data packet including a retransmission indication field. Details are shown in FIG. 38.

[001419] S3801: A sending device obtains a data packet 1 based on a retransmission indication field, context information A, and original data 1, where a value of the context information A is X, and a value of the retransmission indication field is z1.

[001420] The sending device obtains an authentication code A based on the context information A and the original data 1. The sending device concatenates the retransmission indication field, the authentication code A, and the original data 1, to obtain the data packet 1.

[001421] The retransmission indication field whose value is z1 indicates that the data packet 1 is a newly transmitted data packet.

[001422] S3802: The sending device sends the data packet 1 (including the retransmission indication field and the authentication code A) to a receiving device.

[001423] S3803: The receiving device generates an authentication code B based on context information B and the data packet 1, where a value of the context information B is X.

[001424] S3804: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the context information B to X+i.

[001425] S3805: The receiving device sends a success application receipt to the sending device.

[001426] S3806: The sending device updates the value of the context information A to X+i.

[001427] The following describes, with reference to a method in which context information indicates information about a quantity of data packets, another transmission procedure of a data packet including a retransmission indication field. Details are shown in FIG. 39.

[001428] S3901: A sending device obtains a data packet 1 based on a retransmission indication field, context information A, and original data 1, where a value of the context information A is X, and a value of the retransmission indication field is z1.

[001429] The sending device obtains an authentication code A based on the context information A and the original data 1. The sending device concatenates the retransmission indication field, the authentication code A, and the original data 1, to obtain the data packet 1.

[001430] The retransmission indication field whose value is z1 indicates that the data packet 1 is a newly transmitted data packet.

[001431] S3902: The sending device fails to send the data packet 1 (including the retransmission indication field and the authentication code A) to a receiving device.

[001432] The data packet 1 is lost in a transmission process, and therefore the receiving device cannot receive the data packet 1.

[001433] S3903: The sending device obtains a data packet 2 based on a retransmission indication field, the context information A, and the original data 1, where the value of the context information A is X, and a value of the retransmission indication field is z2.

[001434] The sending device obtains the authentication code A based on the context information A and the original data 1. The sending device concatenates the retransmission indication field, the authentication code A, and the original data 1, to obtain the data packet 2.

[001435] The retransmission indication field whose value is z2 indicates that the data packet 2 is

a retransmitted data packet.

[001436] S3904: The sending device sends the data packet 2 (including the retransmission indication field and the authentication code A) to the receiving device.

[001437] S3905: The receiving device generates an authentication code B based on context information B and the data packet 2, where a value of the context information B is X.

[001438] S3906: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the context information B to X+i.

[001439] S3907: The receiving device sends a success application receipt to the sending device.

[001440] S3908: The sending device updates the value of the context information A to X+i.

[001441] In this way, if a data packet is lost in a transmission process, transmission of a next data packet between the sending device and the receiving device is not affected.

[001442] The following describes, with reference to a method in which context information indicates information about a quantity of data packets, another transmission procedure of a data packet including a retransmission indication field. Details are shown in FIG. 40.

[001443] S4001: A sending device obtains a data packet 1 based on a retransmission indication field, context information A, and original data 1, where a value of the context information A is X, and a value of the retransmission indication field is z1.

[001444] The sending device obtains an authentication code A based on the context information A and the original data 1. The sending device concatenates the retransmission indication field, the authentication code A, and the original data 1, to obtain the data packet 1.

[001445] The retransmission indication field whose value is z1 indicates that the data packet 1 is a newly transmitted data packet.

[001446] S4002: The sending device sends the data packet 1 (including the retransmission indication field and the authentication code A) to a receiving device.

[001447] S4003: The receiving device generates an authentication code B based on context information B and the data packet 1, where a value of the context information B is X.

[001448] S4004: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the context information B to X+i.

[001449] S4005: The receiving device fails to send a success application receipt to the sending device.

[001450] The success application receipt is lost in a transmission process, and therefore the sending device cannot receive the success application receipt.

[001451] S4006: The sending device obtains a data packet 2 based on a retransmission indication field, the context information A, and the original data 1, where the value of the context information A is X, and a value of the retransmission indication field is z2.

[001452] The sending device obtains the authentication code A based on the context information A and the original data 1. The sending device concatenates the retransmission indication field, the authentication code A, and the original data 1, to obtain the data packet 2.

[001453] The retransmission indication field whose value is z2 indicates that the data packet 2 is a retransmitted data packet.

[001454] S4007: The sending device sends the data packet 2 (including the retransmission indication field and the authentication code A) to the receiving device.

[001455] S4008: The receiving device generates an authentication code B based on the context information B and the data packet 2, where the value of the context information B is X+i.

[001456] S4009: The receiving device determines that the authentication code A is different from the authentication code B and the value of the retransmission indication field is z2, and the receiving device generates an authentication code C based on the context information B.

[001457] When the authentication code A is different from the authentication code B, the receiving device determines, based on the retransmission indication field, that the data packet 2 is a retransmitted data packet, and the receiving device subtracts a preset value from the value of the context information B, to obtain context information C that is X. The receiving device generates the authentication code C based on the context information C.

[001458] S4010: The receiving device determines that the authentication code A is the same as the authentication code C, and generates a success application receipt.

[001459] S4011: The receiving device sends a success application receipt to the sending device.

[001460] S4012: The sending device updates the value of the context information A to X+i.

[001461] In this way, when a success application receipt is lost in a transmission process, after receiving a retransmitted data packet, the receiving device may send the success application receipt to the sending device again, to prevent the sending device from sending the retransmitted data packet again.

[001462] The following describes, with reference to a method in which context information indicates information about a quantity of data packets, another transmission procedure of a data packet including a retransmission indication field. Details are shown in FIG. 41.

[001463] S4101: A sending device obtains a data packet 1 based on a retransmission indication field, context information A, and original data 1, where a value of the context information A is X, and a value of the retransmission indication field is z1.

[001464] The sending device obtains an authentication code A based on the context information A and the original data 1. The sending device concatenates the retransmission indication field, the authentication code A, and the original data 1, to obtain the data packet 1.

[001465] The retransmission indication field whose value is z1 indicates that the data packet 1 is

a newly transmitted data packet.

[001466] S4102: The sending device sends the data packet 1 (including the retransmission indication field and the authentication code A) to a receiving device.

[001467] S4103: The receiving device generates an authentication code B based on context information B and the data packet 1, where a value of the context information B is X.

[001468] S4104: The receiving device determines that the authentication code A is the same as the authentication code B, and updates the value of the context information B to X+i.

[001469] S4105: The receiving device fails to send a success application receipt to the sending device.

[001470] The success application receipt is lost in a transmission process, and therefore the sending device cannot receive the success application receipt.

[001471] S4106: The sending device obtains a data packet 2 based on a retransmission indication field, the context information A, and original data 2, where the value of the context information A is X, and a value of the retransmission indication field is z1.

[001472] The sending device obtains an authentication code A based on the context information A and the original data 2. The sending device concatenates the retransmission indication field, the authentication code A, and the original data 2, to obtain the data packet 2.

[001473] The retransmission indication field whose value is z1 indicates that the data packet 2 is a newly transmitted data packet.

[001474] S4107: The sending device sends the data packet 2 (including the retransmission indication field and the authentication code A) to the receiving device.

[001475] S4108: The receiving device generates an authentication code B based on the context information B and the data packet 2, where the value of the context information B is X+i.

[001476] S4109: The receiving device determines that the authentication code A is different from the authentication code B and the value of the retransmission indication field is z1, and the receiving device generates a failure application receipt.

[001477] S4110: The receiving device sends the failure application receipt to the sending device.

[001478] S4111: The sending device updates the value of the context information A to X+i.

[001479] In this way, when a success application receipt is lost in a transmission process, the receiving device may send a failure application receipt to the sending device after receiving a newly transmitted data packet. The sending device may update the value of the context information A based on the failure application receipt.

[001480] This application is not limited to the foregoing embodiments, and further provides the following embodiments. It should be noted that the following embodiments may be used in mutual combination with any one or more of the foregoing embodiments.

[001481] In a possible implementation, after a sending device and a receiving device return from a first transmission system to a second transmission system, the receiving device may send a set application receipt to the sending device. The set application receipt may indicate a data packet successfully received by the receiving device. The set application receipt may include identification information of the successfully received data packet (for example, the identification information may include but is not limited to a message ID field, receiving time of the data packet, context information, a sequence number SN, and the like). The sending device may determine a successfully sent data packet based on the identification information of the data packet.

[001482] Specifically, in an inbound process, after a terminal 100 and a satellite network device 200 return to a second transmission system, the satellite network device 200 may generate and send, to the terminal 100, a set application receipt. The set application receipt may include but is not limited to one or more of identification information such as a message ID field of a successfully received data packet, receiving time of the data packet, context information of the data packet, and a sequence number of the data packet. The terminal 100 may determine, based on the set application receipt, a successfully sent data packet and a data packet that fails to be sent. The terminal 100 may further display success prompt information corresponding to the successfully sent data packet. The success prompt information may be used to prompt a user that a satellite message corresponding to the success prompt information is successfully sent. The terminal 100 may further display failure prompt information corresponding to the data packet that fails to be sent. The failure prompt information may be used to prompt the user that a satellite message corresponding to the failure prompt information fails to be sent. Herein, the set application receipt generated by the satellite network device 200 is also referred to as a second application receipt.

[001483] Specifically, in an outbound process, after the terminal 100 and the satellite network device 200 return to the second transmission system, the terminal 100 may generate and send, to the satellite network device 200, a set application receipt. The set application receipt may include but is not limited to one or more of identification information such as a message ID field of a successfully received data packet, receiving time of the data packet, context information of the data packet, and a sequence number of the data packet. The satellite network device 200 may determine, based on the set application receipt, a successfully sent data packet and a data packet that fails to be sent. The satellite network device 200 may delete the successfully sent data packet. Herein, the set application receipt generated by the terminal 100 is also referred to as a fourth application receipt.

[001484] Optionally, the satellite network device 200 may further retransmit, through the second transmission system, the data packet that fails to be sent.

[001485] This application is not limited to the foregoing embodiments, and further provides the

following embodiments. It should be noted that the following embodiments may be used in mutual combination with any one or more of the foregoing embodiments.

[001486] In a possible implementation, in an inbound process, after sending a first data packet to a satellite network device 200, a terminal 100 may further display first sending time prompt information. The first sending time prompt information may be used to prompt a user time at which the terminal 100 sends the first data packet to the satellite network device 200. The first data packet may include a first authentication code generated based on first information, and the first information may be sending time information or first context information.

[001487] For example, the terminal 100 may display a message detail interface 4300 shown in FIG. 43A. The message detail interface 4300 may include but is not limited to a message box 4301, a sending prompt 4302, and a sending time prompt 4303. The message box 4301 may be used to display content of a satellite message that has been sent by the terminal 100 to the satellite network device 200. Herein, the message box 4301 displays "Hello". The sending prompt 4302 may be used to prompt the user that the terminal 100 has sent, to the satellite network device 200, the content displayed in the message box 4301. For example, the sending prompt 1543 may be a character string "Sent". The sending time prompt 4303 may be used to display the time at which the terminal 100 sends the first data packet to the satellite network device 200, for example, "17:23". For specific descriptions of the message detail interface 4300, refer to the embodiment shown in FIG. 15D. Details are not described herein again.

[001488] Optionally, after receiving a success application receipt, the terminal 100 may further display second sending time prompt information while displaying success prompt information. The second sending time prompt information may be used to prompt the user time at which the satellite message is successfully sent.

[001489] For example, as shown in FIG. 43B, after receiving the success application receipt, the terminal 100 may display a success prompt 4311 and a sending time prompt 4312. The success prompt 4311 may be used to prompt the user that the terminal 100 has successfully sent the message content in the message box 4301. The sending time prompt 4312 may be used to prompt the user the time at which the terminal 100 successfully sends the satellite message.

[001490] Optionally, after receiving a failure application receipt, the terminal 100 may further display second sending time prompt information while displaying failure prompt information. The second sending time prompt information may be used to prompt the user time at which the data packet fails to be sent.

[001491] In a possible implementation, in an outbound process, the terminal 100 may further display receiving prompt information and receiving time prompt information after successfully receiving a third data packet sent by the satellite network device 200. The receiving prompt

information may be used to prompt the user that a satellite message is received. The receiving time prompt information may be used to prompt the user time at which the satellite message is received.

[001492] The following describes a terminal 100 according to an embodiment of this application.

[001493] The terminal 100 may be a mobile phone, a tablet computer, a desktop computer, a laptop computer, a handheld computer, a notebook computer, an ultra-mobile personal computer (ultra-mobile personal computer, UMPC), a netbook, a cellular phone, a personal digital assistant (personal digital assistant, PDA), an augmented reality (augmented reality, AR) device, a virtual reality (virtual reality, VR) device, an artificial intelligence (artificial intelligence, AI) device, a wearable device, a vehicle-mounted device, a smart home device, and/or a smart city device. A specific type of the electronic device is not specially limited in this embodiment of this application.

[001494] FIG. 42 is a schematic diagram of a hardware structure according to an embodiment of this application.

[001495] The following uses the terminal 100 as an example to specifically describe this embodiment. It should be understood that the terminal 100 shown in FIG. 42 is merely an example. The terminal 100 may have more or fewer components than those shown in FIG. 42, may combine two or more components, or may have a different component configuration. Components shown in FIG. 42 may be implemented in hardware including one or more signal processing and/or application-specific integrated circuits, software, or a combination of hardware and software.

[001496] The terminal 100 may include a processor 110, an external memory interface 120, an internal memory 121, a universal serial bus (universal serial bus, USB) interface 130, a charging management module 140, a power management module 141, a battery 142, an antenna 1, an antenna 2, a mobile communication module 150, a wireless communication module 160, an audio module 170, a speaker 170A, a receiver 170B, a microphone 170C, a headset jack 170D, a sensor module 180, a button 190, a motor 191, an indicator 192, a camera 193, a display screen 194, a subscriber identity module (subscriber identity module, SIM) card interface 195, and the like. The sensor module 180 may include a pressure sensor 180A, a gyroscope sensor 180B, a barometric pressure sensor 180C, a magnetic sensor 180D, an acceleration sensor 180E, a distance sensor 180F, an optical proximity sensor 180G, a fingerprint sensor 180H, a temperature sensor 180J, a touch sensor 180K, an ambient light sensor 180L, a bone conduction sensor 180M, and the like.

[001497] It may be understood that the structure illustrated in this embodiment of the present invention does not constitute a specific limitation on the terminal 100. In some other embodiments of this application, the terminal 100 may include more or fewer components than those shown in the figure, may combine some components, may split some components, or may have a different component arrangement. The components shown in the figure may be implemented by hardware, software, or a combination of software and hardware.

[001498] The processor 110 may include one or more processing units. For example, the processor 110 may include an application processor (application processor, AP), a modem processor, a graphics processing unit (graphics processing unit, GPU), an image signal processor (image signal processor, ISP), a controller, a memory, a video codec, a digital signal processor (digital signal processor, DSP), a baseband processor, a neural-network processing unit (neural-network processing unit, NPU), and/or the like. Different processing units may be independent components, or may be integrated into one or more processors.

[001499] A wireless communication function of the terminal 100 may be implemented through the antenna 1, the antenna 2, the mobile communication module 150, the wireless communication module 160, the modem processor, the baseband processor, and the like.

[001500] The antenna 1 and the antenna 2 are configured to transmit and receive electromagnetic wave signals. Each antenna in the terminal 100 may be configured to cover one or more communication frequency bands. Different antennas may be further multiplexed, to improve antenna utilization. For example, the antenna 1 may be multiplexed as a diversity antenna of a wireless local area network. In some other embodiments, the antenna may be used in combination with a tuning switch.

[001501] The mobile communication module 150 may provide a wireless communication solution that is applied to the terminal 100 and that includes 2G/3G/4G/5G or the like. The mobile communication module 150 may include at least one filter, a switch, a power amplifier, a low noise amplifier (low noise amplifier, LNA), and the like. The mobile communication module 150 may receive an electromagnetic wave through the antenna 1, perform processing such as filtering and amplification on the received electromagnetic wave, and transmit a processed electromagnetic wave to the modem processor for demodulation. The mobile communication module 150 may further amplify a signal modulated by the modem processor, and convert an amplified signal into an electromagnetic wave through the antenna 1 for radiation. In some embodiments, at least some functional modules in the mobile communication module 150 may be disposed in the processor 110. In some embodiments, at least some functional modules in the mobile communication module 150 may be disposed in a same component as at least some modules in the processor 110.

[001502] The modem processor may include a modulator and a demodulator. The modulator is configured to modulate a to-be-sent low-frequency baseband signal into a medium-high frequency signal. The demodulator is configured to demodulate a received electromagnetic wave signal into a low-frequency baseband signal. Then, the demodulator transmits the low-frequency baseband signal obtained through demodulation to the baseband processor for processing. The low-frequency baseband signal is processed by the baseband processor and then a processed signal is transmitted to the application processor. The application processor outputs a sound signal through

an audio device (not limited to the speaker 170A, the receiver 170B, and the like), or displays an image or a video through the display screen 194. In some embodiments, the modem processor may be an independent component. In some other embodiments, the modem processor may be independent of the processor 110, and disposed in a same component as the mobile communication module 150 or another functional module.

[001503] The wireless communication module 160 may provide a wireless communication solution that is applied to the terminal 100 and that includes a wireless local area network (such as a wireless fidelity (wireless fidelity, Wi-Fi) network), Bluetooth (bluetooth, BT), a global navigation satellite system (global navigation satellite system, GNSS), a satellite communication module, frequency modulation (frequency modulation, FM), a near field communication (near field communication, NFC) technology, an infrared (infrared, IR) technology, or the like. The wireless communication module 160 may be one or more components integrating at least one communication processing module. The wireless communication module 160 receives an electromagnetic wave through the antenna 2, performs frequency modulation and filtering processing on an electromagnetic wave signal, and sends a processed signal to the processor 110. The wireless communication module 160 may further receive a to-be-sent signal from the processor 110, perform frequency modulation and amplification on the signal, and convert a modulated and amplified signal into an electromagnetic wave through the antenna 2 for radiation.

[001504] The satellite communication module may be configured to communicate with a satellite network device. In a satellite communication system, the satellite communication module may communicate with a satellite network device 200, and the satellite communication module can support data packet transmission with the satellite network device 200. For example, when the satellite communication system is a BeiDou communication system, the satellite network device 200 is a BeiDou network device 200, the satellite communication module may communicate with the BeiDou network device 200, and the satellite communication module can support BeiDou short packet (a data packet in the BeiDou communication system) transmission with the BeiDou network device 200.

[001505] In some embodiments, the antenna 1 of the terminal 100 is coupled to the mobile communication module 150, and the antenna 2 is coupled to the wireless communication module 160, so that the terminal 100 can communicate with a network and another device by using a wireless communication technology. The wireless communication technology may include a global system for mobile communications (global system for mobile communications, GSM), a general packet radio service (general packet radio service, GPRS), code division multiple access (code division multiple access, CDMA), wideband code division multiple access (wideband code division multiple access, WCDMA), time-division code division multiple access (time-division

code division multiple access, TD-CDMA), long term evolution (long term evolution, LTE), BT, a GNSS, a WLAN, NFC, FM, an IR technology, and/or the like. The GNSS may include a global positioning system (global positioning system, GPS), a global navigation satellite system (global navigation satellite system, GLONASS), a BeiDou navigation satellite system (beidou navigation satellite system, BDS), a quasi-zenith satellite system (quasi-zenith satellite system, QZSS), and/or a satellite based augmentation system (satellite based augmentation system, SBAS).

[001506] The terminal 100 implements a display function through the GPU, the display screen 194, the application processor, and the like. The GPU is a microprocessor for image processing, and is connected to the display screen 194 and the application processor. The GPU is configured to: perform mathematical and geometric computation, and render an image. The processor 110 may include one or more GPUs, and execute program instructions to generate or change display information.

[001507] The display screen 194 is configured to display an image, a video, or the like. The display screen 194 includes a display panel. In some embodiments, the terminal 100 may include one or N display screens 194, where N is a positive integer greater than 1. The pressure sensor 180A is configured to sense a pressure signal, and can convert the pressure signal into an electrical signal. In some embodiments, the pressure sensor 180A may be disposed on the display screen 194. The touch sensor 180K is also referred to as a "touch panel". The touch sensor 180K is configured to detect a touch operation acting on or near the touch sensor. The touch sensor may transfer the detected touch operation to the application processor to determine a touch event type. Visual output related to the touch operation may be provided through the display screen 194.

[001508] The SIM card interface 195 is configured to be connected to a SIM card. The SIM card may be inserted into the SIM card interface 195 or pulled out from the SIM card interface 195, to implement contact with or separation from the terminal 100. The terminal 100 may support one or N SIM card interfaces, where N is a positive integer greater than 1. The SIM card interface 195 may support a nano-SIM card, a micro-SIM card, a SIM card, and the like. A plurality of cards may be simultaneously inserted into a same SIM card interface 195. The plurality of cards may be of a same type or different types. The SIM card interface 195 may also be compatible with different types of SIM cards. The SIM card interface 195 may also be compatible with an external storage card. The terminal 100 interacts with a network through the SIM card, to implement functions such as calling and data communication. In some embodiments, the terminal 100 uses an eSIM, namely, embedded SIM card. The eSIM card may be embedded in the terminal 100, and cannot be separated from the terminal 100.

[001509] In conclusion, the foregoing embodiments are merely intended for describing the technical solutions of this application, but not for limiting this application. Although this

application is described in detail with reference to the foregoing embodiments, persons of ordinary skill in the art should understand that they may still make modifications to the technical solutions described in the foregoing embodiments or make equivalent replacements to some technical features thereof, without departing from the scope of the technical solutions of embodiments of this application.

[001510] It may be understood that the foregoing embodiments may be used in mutual combination. For example, when the information A of the sending device is context information A and the information B of the receiving device is context information B, and the context information A and the context information B of the sending device and the receiving device are inconsistent, the sending device may set the information A to sending time information, and the receiving device may set the information B to receiving time information. In this way, the sending device and the receiving device may continue to communicate with each other in the first transmission system. It should be further noted that a combination manner is not limited to the foregoing described combination manner, and the combination manner is not limited in embodiments of this application.

CLAIMS

What is claimed is:

1. A transmission method, comprising:

generating a first authentication code based on first information, a first key, and first data, wherein the first information is sending time information or first context information;

generating a first data packet based on the first authentication code and the first data; and

sending the first data packet in a first transmission system.

2. The method according to claim 1, wherein before the generating a first authentication code based on first information, a first key, and first data, the method further comprises:

obtaining the first key, wherein the first key is obtained by a first device through negotiation with a second device in a second transmission system, and the first transmission system is different from the second transmission system.

3. The method according to claim 1, wherein before the generating a first authentication code based on first information, a first key, and first data, the method further comprises:

establishing a communication connection to a fourth device; and

obtaining the first key through the fourth device.

4. The method according to claim 2, wherein the second transmission system is a cellular transmission system or a wireless local area network WLAN transmission system, and the first transmission system is a satellite transmission system.

5. The method according to any one of claims 1 to 4, wherein the sending, by the first device, the first data packet to a second device in a first transmission system specifically comprises:

after processing the first data packet into at least one second data packet at a message data convergence protocol MDCP layer of a first device and/or a satellite link control SLC layer of the first device, sending the at least one second data packet to a second device through a third device.

6. The method according to any one of claims 1 to 5, wherein the sending time information indicates sending time of the first data packet.

7. The method according to claim 6, wherein time at which a first device sends the first data packet is time at which an application AP layer of the first device sends the first data packet to the message data convergence protocol MDCP layer, or is time estimated by the first device for sending the first data packet to a second device.

8. The method according to any one of claims 1 to 7, wherein after the sending the first data packet to a second device in a first transmission system, the method further comprises:

displaying sending prompt information, wherein the sending prompt information prompts the user that the first device has sent the first data packet to the second device.

9. A secure transmission method, comprising:

receiving, in a first transmission system, a first data packet sent by a first device;

generating a second authentication code based on second information, a first key, and the first data packet, wherein the second information is receiving time information or second context information; and

determining a receiving status of the first data packet based on the second authentication code.

10. The method according to claim 9, wherein before the generating a second authentication code based on second information, a first key, and the first data packet, the method further comprises:

obtaining the first key, wherein the first key is obtained by a second device through negotiation with a first device in a second transmission system, and the second transmission system is different from the first transmission system.

11. The method according to claim 10, wherein the second transmission system is a cellular transmission system or a WLAN transmission system, and the first transmission system is a satellite transmission system.

12. The method according to any one of claims 9 to 11, wherein the receiving, in a first transmission system, a first data packet specifically comprises:

receiving, in the first transmission system, the first data packet sent by a third device.

13. The method according to any one of claims 9 to 12, wherein the second device determines a first authentication code based on the first data packet.

14. The method according to any one of claims 9 to 13, wherein before the generating a second authentication code based on second information, a first key, and the first data packet, the method further comprises:

receiving the second information sent by the third device.

15. A transmission method, comprising:

receiving at least one second data packet;

generating a first data packet based on the at least one second data packet; and

sending the first data packet.

16. The method according to claim 15, wherein the method further comprises:

sending second information or fourth information to a second device, wherein the second information or the fourth information is receiving time information.

17. The method according to claim 16, wherein the receiving time information indicates corresponding time at which the third device receives the 1st data packet in the at least one second data packet.

18. A communication apparatus, comprising one or more processors and one or more

memories, wherein the one or more memories are configured to store computer program code, the computer program code comprises computer instructions, and when the one or more processors execute the computer instructions, the communication apparatus is enabled to perform the method according to any one of claims 1 to 17.

19. A computer-readable storage medium, wherein the computer-readable storage medium stores instructions, and when the instructions are run on a computer, the computer is enabled to perform the method according to any one of claims 1 to 17.