COMMUNICATION METHOD AND APPARATUS

TECHNICAL FIELD

[0002] Embodiments of this application relate to the field of communication technologies, and in particular, to a communication method and apparatus.

BACKGROUND

[0003] Vehicle to everything (vehicle to everything, V2X) is a key technology in an intelligent transportation system, and is considered to be one of fields that have the most industry potential and most definite market requirements in an internet of things system. Vehicle to everything is usually a communication network that provides vehicle information by using sensors installed on vehicles, vehicle-mounted terminals, or the like, and implements vehicle to vehicle (vehicle to vehicle, V2V) communication, vehicle to infrastructure (vehicle to infrastructure, V2I) communication, vehicle to network (vehicle to network, V2N) communication, and vehicle to pedestrian (vehicle to pedestrian, V2P) communication. Usually, in a V2X scenario, a communication link for direct communication between a terminal and another terminal may be referred to as a sidelink (sidelink, SL), and an SL interface may be referred to as a PC5 interface.

[0004] In new radio (new radio, NR) V2X, high-reliability services between terminals impose higher requirements on communication quality. How to ensure correct communication between terminals is a problem that needs to be resolved currently.

SUMMARY

[0005] Embodiments of this application provide a communication method and apparatus, to ensure correct

control at the application layer.

[0053] The RRC layer is configured to support functions such as radio resource management and RRC connection control.

[0054] For definitions and functions of other protocol layers such as the PDCP layer and the RLC layer, refer to descriptions in a conventional technology. Details are not described herein.

[0055] FIG. 3 is a schematic flowchart of updating a key between two terminals in a unicast connection. The method includes the following steps.

[0056] Step 301: A first terminal sends a key update request message to a second terminal. Correspondingly, the second terminal may receive the key update request message.

[0057] The key update request message is used to request to update a key of a unicast connection. The key update request message may be, for example, a DirectRekeyRequest message.

[0058] The key update request message carries security capability information of the first terminal, a key update request indication, and eight most significant bits of a new key identifier. The security capability information includes a security algorithm that can be supported by the first terminal in the unicast connection. The security algorithm herein includes an integrity protection algorithm and/or a ciphering algorithm.

[0059] It should be noted that, in a key update procedure between the first terminal and the second terminal, the first terminal sends the key update request message to the second terminal to obtain a 256-bit new key, where the new key may be identified by using an identifier of the new key (also referred to as the new key identifier). The new key identifier has 16 bits, where the eight most significant bits are confirmed by the first terminal in advance, and eight least significant bits are confirmed by the second terminal. The first terminal sends the eight most significant bits of the new key identifier to the second terminal, and the second terminal sends the eight least significant bits of the new key identifier to the first terminal, so that both the first terminal and the second terminal can obtain the new key identifier.

[0060] Step 302: The second terminal selects a new security algorithm, and determines the new key.

[0061] The second terminal selects, based on the security capability information of the first terminal, an integrity protection algorithm from one or more integrity protection algorithms supported by the first terminal, and/or a ciphering algorithm from one or more ciphering algorithms supported by the first terminal. Then, the second terminal determines the new key based on the selected integrity protection algorithm and/or the selected ciphering algorithm.

[0062] After determining the new key, the second terminal establishes a security context of the new key. Subsequently, the second terminal may start to receive, from the first terminal, data ciphered by using the new key on the unicast connection. Alternatively, it is understood that the second terminal enables a function of receiving, from

the first terminal, data ciphered by using the new key on the unicast connection.

[0063] It should be noted that a plurality of unicast connections may be established between the first terminal and the second terminal, and one key is used for each unicast connection. The new key negotiated between the first terminal and the second terminal is for one of the unicast connections.

[0064] Step 303: The second terminal sends a security mode command message to the first terminal. Correspondingly, the first terminal may receive the security mode command message.

[0065] The security mode command message may be, for example, a DirectSecurityModeCommand message.

[0066] The security mode command message carries indications/an indication of the new integrity protection algorithm and/or the new ciphering algorithm selected by the second terminal, the security capability information of the first terminal, and the eight least significant bits of the new key identifier.

[0067] Step 304: The first terminal determines the new key.

[0068] The first terminal first performs integrity verification on the received security mode command message, and verifies the carried security capability information of the first terminal. When all verification results are correct, the first terminal obtains the new key based on the new integrity protection algorithm and/or the new ciphering algorithm indicated in the security mode command message and according to a key derivation method that is the same as that used by the second terminal, where the new key is the same as the new key derived by the second terminal.

[0069] After determining the new key, the first terminal establishes a security context of the new key, determines that data ciphered by using the new key may be subsequently received from the second terminal on the unicast connection, and may cipher, by using the new key, data that needs to be sent to the second terminal on the unicast connection. Alternatively, it is understood that the second terminal enables a function of receiving, from the first terminal on the unicast connection, data ciphered by using the new key, and enables a function of ciphering, by using the new key, data that needs to be sent to the second terminal on the unicast connection.

[0070] Step 305: The first terminal sends a security mode complete message to the second terminal. Correspondingly, the second terminal may receive the security mode complete message.

[0071] The security mode complete message may be, for example, a DirectSecurityModeComplete message, used to indicate that the first terminal has completed the key updating.

[0072] The second terminal performs integrity verification on the received security mode complete message. When a verification result is correct, the second terminal confirms that the key of the first terminal is correctly updated.

[0073] After confirming that the key of the first terminal is correctly updated, the second terminal determines that the new key can be subsequently used to cipher data that needs to be sent to the first terminal on the unicast connection. Alternatively, it is understood that the second terminal enables a function of ciphering, by using the new

of the first terminal, where the second indication indicates to re-establish a PDCP entity configured to send data or indicates that the PDCP layer can use the new key to process to-be-sent data on the unicast connection.

[0099] The second indication indicates that the PDCP layer can use the new key to process the to-be-sent data on the unicast connection, or may be understood as indicating that the PDCP layer can send data, on the unicast connection, ciphered by using the new key, or may be understood as indicating that the PDCP layer can use the new key to cipher and send data that needs to be sent on the unicast connection, or may be understood as indicating that the PDCP layer has a capability of processing the to-be-sent data on the unicast connection by using the new key.

[00100] Specifically, the second indication may be a capability indication that is of processing the to-be-sent data by using the new key and that is sent by the application layer of the first terminal to the access stratum of the first terminal, to trigger the application layer of the first terminal to apply the new key and the new integrity protection and ciphering algorithms, so that the first terminal has a capability of processing the to-be-sent data on the unicast connection by using the new key. Alternatively, the application layer of the first terminal may send, to the access stratum of the first terminal, a re-establishment indication of the PDCP entity that is related to the unicast connection and that sends data. In a process of re-establishing the PDCP entity that receives data, the new key and the new integrity protection and ciphering algorithms are applied, so that the first terminal has a capability of processing the to-be-sent data on the unicast connection by using the new key.

[00101] The PDCP entity configured to send data is associated with the unicast connection between the first terminal and the second terminal. Alternatively, it is understood that there may be a plurality of unicast connections between the first terminal and the second terminal, and the PDCP entity configured to send data is associated with one of the unicast connections. When there are a plurality of unicast connections, different PDCP entities need to be associated with different unicast connections.

[00102] It should be noted that the PDCP entity configured to send data and the PDCP entity configured to receive data in this embodiment are associated with a same unicast connection.

[00103] That the application layer of the first terminal sends a second indication to the access stratum may be, for example, that the application layer sends the second indication to the PDCP layer. Alternatively, the application layer may send the second indication to the RRC layer. After receiving the second indication, the RRC layer may indicate the PDCP layer to re-establish the PDCP entity configured to send data. Specifically, the PDCP entity that is used to cipher and send, by using the new key, data that needs to be sent on the unicast connection is re-established.

[00104] In an implementation method, that after the first terminal receives the data ciphered by using the new key may be, for example, that after the first terminal receives a security mode complete message (for example, the message in step 305 in the embodiment in FIG. 3) from the second terminal.

purpose processor may be a microprocessor. Optionally, the general-purpose processor may alternatively be any conventional processor, controller, microcontroller, or state machine. The processor may also be implemented by a combination of computing apparatuses, such as a digital signal processor and a microprocessor, a plurality of microprocessors, one or more microprocessors with a digital signal processor core, or any other similar configuration.

[00176] Steps of the methods or algorithms described in embodiments of this application may be directly embedded into hardware, a software unit executed by a processor, or a combination thereof. The software unit may be stored in a random access memory (Random Access Memory, RAM), a flash memory, a read-only memory (Read-Only Memory, ROM), an EPROM memory, an EEPROM memory, a register, a hard disk, a removable magnetic disk, a CD-ROM, or a storage medium of any other form in the art. For example, the storage medium may connect to a processor so that the processor may read information from the storage medium and write information to the storage medium. Optionally, the storage medium may alternatively be integrated into a processor. The processor and the storage medium may be disposed in the ASIC.

[00177] These computer program instructions may alternatively be loaded onto a computer or another programmable data processing device, so that a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or the another programmable device provide steps for implementing a specific function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[00178] A person skilled in the art should be aware that in the foregoing one or more examples, functions described in this application may be implemented by hardware, software, firmware, or any combination thereof. When the functions are implemented by software, the foregoing functions may be stored in a computer-readable medium or transmitted as one or more instructions or code in a computer-readable medium. The computer-readable medium includes a computer storage medium and a communication medium, where the communication medium includes any medium that enables a computer program to be transmitted from one place to another. The storage medium may be any available medium accessible to a general-purpose or special-purpose computer.

[00179] Although this application is described with reference to specific features and embodiments thereof, it is clear that various modifications and combinations may be made to them without departing from the scope of this application. Correspondingly, the specification and accompanying drawings are merely example description of this application defined by the appended claims, and are considered as any of or all modifications, variations, combinations or equivalents that cover the scope of this application. It is clearly that, a person skilled in the art can make various modifications and variations to this application without departing from the scope of this application. This application is intended to cover these modifications and variations of this application provided that they fall

CLAIMS

1. A communication method, comprising:

receiving, by a first terminal, a first data packet from a second terminal, wherein the first data packet carries a key identifier, and a key corresponding to the key identifier is used for communication on a unicast connection between the first terminal and the second terminal; and

discarding, by the first terminal, the first data packet if the first terminal does not store a key security context corresponding to the key identifier.

2. The method according to claim 1, wherein the method further comprises:performing, by a first terminal, integrity protection verification on a received radio resource control, RRC, message; and

when the integrity protection verification fails, sending, by an RRC layer of the first terminal, a first indication and an identifier of a second terminal to an application layer of the first terminal, wherein the first indication and the identifier of the second terminal are used by the application layer to disconnect a unicast connection between the first terminal and the second terminal.

3. The method according to claim 2, wherein the method further comprises:

disconnecting, by the RRC layer of the first terminal, an RRC connection between the first terminal and the second terminal, wherein

the first indication is an RRC connection disconnection indication, which indicates that the RRC connection between the first terminal and the second terminal is disconnected.

4. The method according to claim 2, wherein the first indication is an integrity protection verification failure indication, which indicates that the integrity protection verification performed by the first terminal on the RRC message received from the second terminal fails.

5. The method according to any one of claims 2 or 3, wherein the method further comprises:

updating, by the application layer of the first terminal, a layer 2 identifier of the first terminal.

6. The method according to any one of claims 2 to 4, wherein the method further comprises:

re-establishing, by the first terminal, the unicast connection to the second terminal by using a new key.

7. The method according to any one of claims 2 to 5, wherein the method further comprises:

sending, by the first terminal, sidelink information to a network device, wherein the sidelink information comprises a second indication and the identifier of the second terminal, and the second indication indicates that a radio link failure occurs on the unicast connection between the first terminal and the second terminal and a failure cause is that the integrity protection verification performed on the RRC message received from the second terminal fails.

8. The method according to any one of claims 2 to 7, wherein the application layer comprises a PC5-S layer or a V2X layer.

9. A communication apparatus, comprising modules for carrying out steps of the method according to any one of claims 1 to 8.

10. A computer-readable storage medium, comprising a computer program, wherein when the computer program runs on a computer, the computer is enabled to perform the communication method according to any one of claims 1 to 8.

11. A computer program product, wherein the computer program product comprises a computer program; and when the computer program runs, the communication method according to any one of claims 1 to 8 is enabled to be performed.

12. A communication system, comprising the communication apparatus according to any one of claims 1 to 8.

13. The system according to claim 12, wherein the system further comprises a second terminal.

14. The system according to claim 12 or 13, wherein the system further comprises a network device.