## 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,

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.

2. The method according to claim 1, 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.

3. The method according to claim 1, 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.

4. The method according to any one of claims 1 or 2, wherein the method further comprises:

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

5. The method according to any one of claims 1 to 3, wherein the method further comprises:

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

6. The method according to any one of claims 1 to 4, 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.

7. The method according to any one of claims 1 to 6, wherein the application layer comprises a PC5-S layer or a V2X layer.

8. A communication apparatus, comprising modules for carrying out steps of the method according to any one of claims 1 to 7.

9. 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 7.

10. 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 7 is enabled to be performed.

11. A communication system, comprising the communication apparatus according to any one of claims 1 to 7.

12. The system according to claim 11, wherein the system further comprises a second terminal.

13. The system according to claim 11 or 12, wherein the system further comprises a network device.