CLAIMS

1. A communication method, comprising:

obtaining, by a first communication apparatus, a security policy corresponding to a proximity-based services group, wherein the security policy comprises a confidentiality security policy and/or an integrity security policy, the confidentiality security policy indicates whether confidentiality security protection is enabled for a message of the proximity-based services group, the integrity security policy indicates whether integrity security protection is enabled for the message of the proximity-based services group, the proximity-based services group comprises at least two members, and the first communication apparatus is one of the at least two members;

determining, by the first communication apparatus according to the security policy, whether to perform security protection on a payload field carried in a to-be-sent first message, and assigning a value to a field other than the payload field in the first message, wherein the field other than the payload field comprises one or more of the following: an identifier of a proximity-based services group key, an identifier of a proximity-based services group traffic key, a freshness parameter, confidentiality indication information, integrity indication information, or a message authentication code, MAC, the confidentiality indication information indicates whether the confidentiality security protection is enabled, the integrity indication information indicates whether the integrity security protection is enabled, and the security protection comprises the confidentiality security protection and/or the integrity security protection; and

sending, by the first communication apparatus, the first message to a second communication apparatus.

2. The method according to claim 1, wherein the assigning the value to the field other than the payload field in the first message comprises:

when the confidentiality security policy indicates that the confidentiality security protection is not enabled, but the integrity security policy indicates that the integrity security protection is enabled, setting, by the first communication apparatus, the MAC not to be 0, and setting at least one of the identifier of the proximity-based services group key, the identifier of the proximity-based services group traffic key, and the freshness parameter not to be 0.

3. The method according to claim 1 or 2, wherein the assigning the value to the field other than the payload field in the first message comprises:

when the confidentiality security policy indicates that the confidentiality security protection is not enabled, but the integrity security policy indicates that the integrity security protection is enabled, setting, by the first communication apparatus, the confidentiality indication information to be 0.

4. The method according to claim 1, wherein the determining, by the first communication apparatus according to the security policy, whether to perform security protection on the payload field carried in the to-be-sent first message, and assigning the value to the field other than the payload field in the first message comprise one or more of the following:

when the confidentiality security policy indicates that the confidentiality security protection is enabled, determining, by the first communication apparatus, to perform confidentiality security protection on the payload field carried in the to-be-sent first message, and setting a value of at least one of the identifier of the proximity-based services group key, the identifier of the proximity-based services group traffic key, the freshness parameter, and the confidentiality indication information that are carried in the first message not to be 0;

when the integrity security policy indicates that the integrity security protection is enabled, determining, by the first communication apparatus, to perform integrity security protection on the payload field carried in the to-be-sent first message, and setting a value of the MAC carried in the first message not to be 0;

when the confidentiality security policy indicates that the confidentiality security protection is not enabled, determining, by the first communication apparatus, not to perform confidentiality security protection on the payload field carried in the to-be-sent first message, and setting a value of at least one of the identifier of the proximity-based services group key, the identifier of the proximity-based services group traffic key, the freshness parameter, and the confidentiality indication information that are carried in the first message to be 0; or

when the integrity security policy indicates that the integrity security protection is not enabled, determining, by the first communication apparatus, not to perform integrity security protection on the payload field carried in the to-be-sent first message, and setting a value of the MAC carried in the first message to be 0.

5. The method according to any one of claims 1 to 4, wherein the determining, by the first communication apparatus according to the security policy, whether to perform security protection on the payload field carried in the to-be-sent first message, and assigning the value to the field other than the payload field in the first message comprise:

determining, by the first communication apparatus according to a local policy and the security policy, to perform security protection on the payload field carried in the first message, and assigning the value to the field other than the payload field in the first message, wherein the local policy indicates a trigger condition for the first communication apparatus to perform security protection on the payload field.

6. The method according to claim 5, wherein the determining, by the first communication apparatus according to the local policy and the security policy, to perform security protection on

the payload field, and assigning the value to the field other than the payload field in the first message comprise:

when the security policy indicates that the security protection is optionally enabled, determining, by the first communication apparatus according to the local policy, to perform security protection on the payload field, and assigning the value to the field other than the payload field in the first message.

7. The method according to claim 5 or 6, wherein the determining, by the first communication apparatus according to the local policy and the security policy, to perform security protection on the payload field, and assigning the value to the field other than the payload field in the first message comprise one or more of the following:

when the confidentiality security policy indicates that the confidentiality security protection is optionally enabled, and a type of the first communication apparatus is a roadside unit, determining, by the first communication apparatus, not to perform confidentiality security protection on the payload field, and setting a value of the confidentiality indication information carried in the field other than the payload field to be 0, or setting the at least one of the identifier of the proximity-based services group key, the identifier of the proximity-based services group traffic key, and the freshness parameter to be 0; or

when the confidentiality security policy indicates that the confidentiality security protection is optionally enabled, and a type of the first communication apparatus is a vehicle, determining, by the first communication apparatus, to perform confidentiality security protection on the payload field, and setting a value of the confidentiality indication information carried in the field other than the payload field not to be 0, or setting the at least one of the identifier of the proximity-based services group key, the identifier of the proximity-based services group traffic key, and the freshness parameter not to be 0.

8. The method according to claim 1, wherein the determining, by the first communication apparatus according to the security policy, whether to perform security protection on the payload field carried in the to-be-sent first message, and assigning the value to the field other than the payload field in the first message comprise:

when the confidentiality security policy indicates that the confidentiality security protection is not enabled, and the integrity security policy indicates that the integrity security protection is not enabled, setting, by the first communication apparatus, at least one of the identifier of the proximity-based services group key, the identifier of the proximity-based services group traffic key, and the freshness parameter not to be 0.

9. The method according to any one of claims 1 to 8, wherein the confidentiality indication information is carried in an information header of a packet data convergence protocol PDCP data

packet of the first communication apparatus.

10. The method according to any one of claims 1 to 9, wherein the obtaining, by the first communication apparatus, the security policy corresponding to the proximity-based services group comprises:

sending, by the first communication apparatus, a request message to a key management function network element, wherein the request message comprises a group identifier of the proximity-based services group and a security capability of the first communication apparatus, and the request message is used to request to obtain the security policy associated with the group identifier; and

receiving, by the first communication apparatus, the security policy from the key management function network element.

11. A communication method, comprising:

receiving, by a second communication apparatus, a first message from a first communication apparatus, wherein the first message comprises a payload field and a field other than the payload field, the field other than the payload field comprises a message authentication code, MAC; and

determining, by the second communication apparatus according to an integrity security policy corresponding to a proximity-based services group, whether to perform integrity check on the payload field, wherein the integrity security policy indicates whether integrity security protection is enabled for a message of the proximity-based services group, the proximity-based services group comprises at least two members, the second communication apparatus is one of the at least two members.

12. The method according to claim 11, wherein the determining, by the second communication apparatus according to the integrity security policy corresponding to the proximity-based services group, whether to perform integrity check on the payload field comprises:

when the integrity security policy indicates that the integrity security protection is enabled, determining, by the second communication apparatus, to perform integrity check on the payload field.

13. The method according to claim 11 or 12, wherein the determining, by the second communication apparatus according to the integrity security policy corresponding to the proximity-based services group, whether to perform integrity check on the payload field comprises:

determining, by the second communication apparatus according to the integrity security policy and the field other than the payload field, whether to perform integrity check on the payload field.

14. The method according to claim 13, wherein the determining, by the second communication apparatus according to the integrity security policy and the field other than the

payload field, whether to perform integrity check on the payload field comprises:

when the integrity security policy indicates that the integrity security protection is enabled, and the field other than the payload field does not carry the MAC or a value of the MAC carried in the field other than the payload field is 0, discarding, by the second communication apparatus, the first message.

15. The method according to claim 13, wherein the determining, by the second communication apparatus according to the integrity security policy and the field other than the payload field, whether to perform integrity check on the payload field comprises:

when the integrity security policy indicates that the integrity security protection is optionally enabled, and the field other than the payload field does not carry the MAC or the value of the MAC carried in the field other than the payload field is 0, determining, by the second communication apparatus, not to perform integrity check on the payload field.

16. The method according to any one of claims 11 to 15, wherein the method further comprises:

sending, by the second communication apparatus, a request message to a key management function network element, wherein the request message comprises a group identifier of the proximity-based services group and a security capability of the second communication apparatus, and the request message is used to request to obtain the integrity security policy associated with the group identifier; and

receiving, by the second communication apparatus, the integrity security policy from the key management function network element.

17. A communication apparatus, configured to perform the method according to any one of claims 1 to 16.

18. A computer-readable storage medium, wherein the computer-readable storage medium stores a computer program, and when the computer program is run, the computer is enabled to perform the method according to any one of claims 1 to 16.