

COMMUNICATION METHOD AND COMMUNICATION APPARATUS

ABSTRACT

Embodiments of this application provide a communication method and apparatus. The method includes: A first communication apparatus obtains a security policy corresponding to a proximity-based services group; determines, according to the security policy, whether to perform security protection on a payload field carried in a first message, and assigns a value to a field other than the payload field in the first message; and sends the first message to a second communication apparatus. The field other than the payload field includes at least one 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. The confidentiality indication information indicates whether confidentiality security protection is enabled, and the integrity indication information indicates whether integrity security protection is enabled. The first communication apparatus is one of at least two members in the proximity-based services group. The technical solutions of this application can prevent the second communication apparatus from being spoofed, and reduce potential security risks.

FIG. 3