

COMMUNICATION METHOD AND RELATED APPARATUS

ABSTRACT

A communication method and a related apparatus are provided, and are applied to the fields of communication technologies and intelligent vehicles. The method includes: receiving a first message from a first node, where the first message includes a first key agreement parameter, the first key agreement parameter is obtained based on a first private key and an intermediate parameter, the intermediate parameter is obtained based on a security parameter and a common parameter, and the security parameter is a first password or a PSK; determining a first key based on the first key agreement parameter and a second private key; sending a second message to the first node, where the second message includes a second key agreement parameter, and the second key agreement parameter is obtained based on the second private key and the intermediate parameter; and obtaining the first key based on the first key agreement parameter and the second private key. According to embodiments of this application, security of a shared key can be improved, access of an untrusted attacker can be avoided, and node security can be improved.

(Fig.4)