ABSTRACT

ENCRYPTION KEY DISTRIBUTION SYSTEM

The encryption key distribution system includes a node **A**, a node **B**, and an authentication server **S**. Upon receiving a first nonce created by the node **A** and a second nonce created by the node **B**, the authentication server **S** creates a session key. The authentication server **S** sends a first message authentication code value and a first encryption message to the node **A**. The first encryption message is created by encrypting the first nonce, the session key, and first additional information with a first secret key. The authentication server **S** sends a second message authentication code value and a second encryption message to the node **B**. The second encryption message is created by encrypting the second nonce, the session key, and second additional information with a second secret key. The node **A** decrypts the first encryption message with the first secret key, thereby obtaining the session key and the first additional information. Further, the node **A** authenticates the session key by use of the first message authentication code value. The node **B** decrypts the second encryption message with the second secret key, thereby obtaining the session key and the second additional information. Further, the node **B** authenticates the session key by use of the second message authentication code value.

(Figure 1)