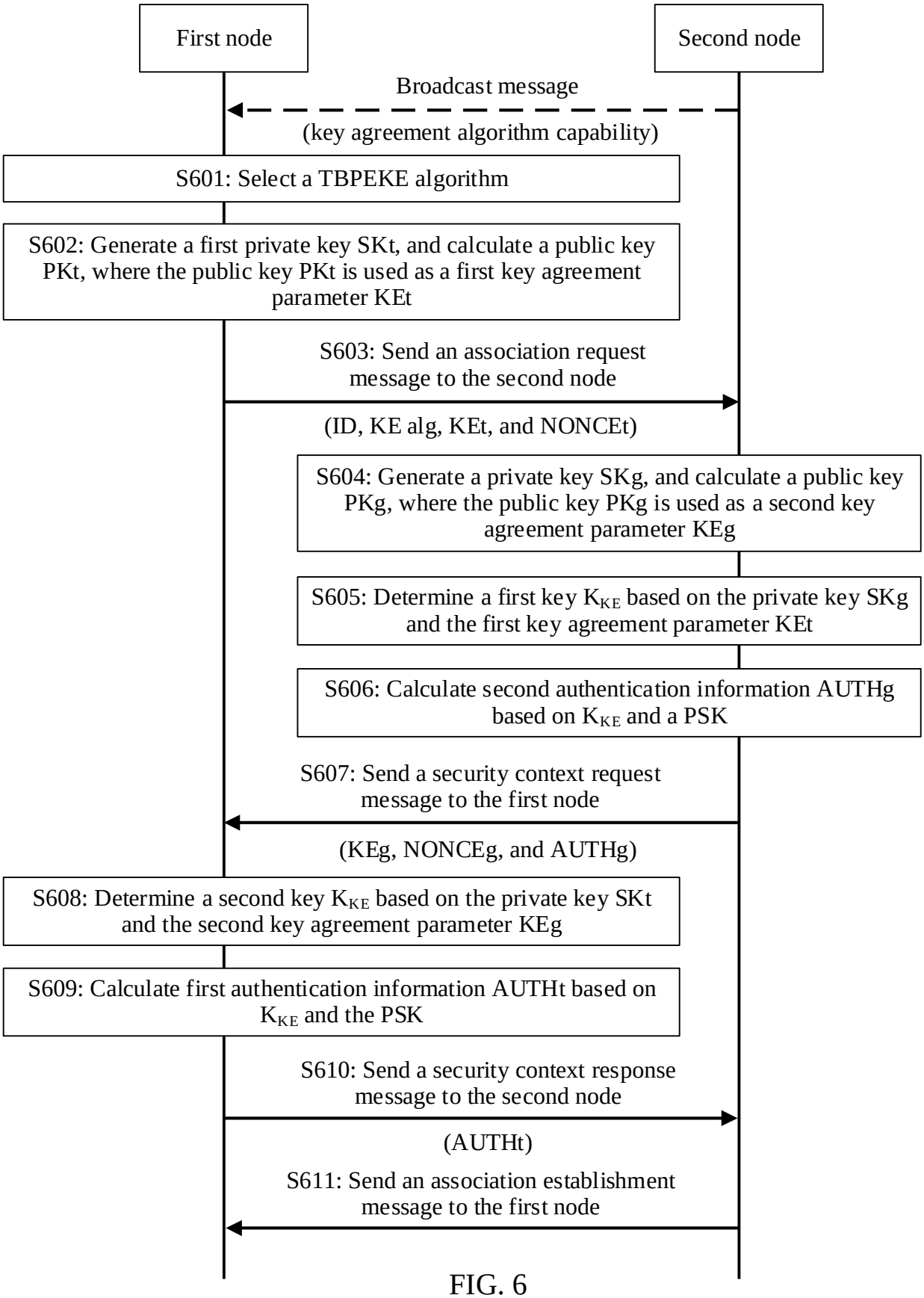

First node
Second node
Broadcast message
(key agreement algorithm capability)
S601: Select a TBPEKE algorithm
S602: Generate a first private key SKt, and calculate a public key PKt, where the public key PKt is used as a first key agreement parameter KEt
S603: Send an association request message to the second node
(ID, KE alg, KEt, and NONCEt)
S604: Generate a private key SKg, and calculate a public key PKg, where the public key PKg is used as a second key agreement parameter KEg
S605: Determine a first key K_{KE} based on the private key SKg and the first key agreement parameter KEt
S606: Calculate second authentication information AUTHg based on K_{KE} and a PSK
S607: Send a security context request message to the first node
(KEg, NONCEg, and AUTHg)
S608: Determine a second key K_{KE} based on the private key SKt and the second key agreement parameter KEg
S609: Calculate first authentication information AUTHt based on K_{KE} and the PSK
S610: Send a security context response message to the second node
(AUTHt)
S611: Send an association establishment message to the first node

FIG. 6