World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:8, No:04, 2014

Proposed Terminal Device for End-to-End Secure SMS in Cellular Networks

Authors : Neetesh Saxena, Narendra S. Chaudhari

Abstract : Nowadays, SMS is a very popular mobile service and even the poor, illiterate people and those living in rural areas use SMS service very efficiently. Although many mobile operators have already started 3G and 4G services, 2G services are still being used by the people in many countries. In 2G (GSM), only encryption provided is between the MS and the BTS, there is no end-to-end encryption available. Sometimes we all need to send some confidential message to other person containing bank account number, some password, financial details, etc. Normally, a message is sent in plain text only to the recipient and it is not an acceptable standard for transmitting such important and confidential information. Authors propose an end-to-end encryption approach by proposing a terminal for sending/receiving a secure message. An asymmetric key exchange algorithm is used in order to transmit secret shared key securely to the recipient. The proposed approach with terminal device provides authentication, confidentiality, integrity and non-repudiation.

Keywords : AES, DES, Diffie-Hellman, ECDH, A5, SMS
Conference Title : ICITCS 2014 : International Conference on Information Technology and Computer Science
Conference Location : Venice, Italy
Conference Dates : April 14-15, 2014