Abstract

Wireless body area network (WBANs) is composed of sensors that collect and transmit a person's physiological data to health-care providers in real-time. In order to guarantee security of this data over open networks, a secure data transmission mechanism between WBAN and application provider's servers is of necessity. Modified medical data does not provide a true reflection of an individuals state of health and its subsequent use for diagnosis could lead to an irreversible medical condition. In this paper, we propose a lightweight certificateless signcryption scheme for secure transmission of data between WBAN and servers. Our proposed scheme not only provides confidentiality of data and authentication in a single logical step, it is lightweight and resistant to key escrow attacks. We further provide security proof that our scheme provides indistinguishability against adaptive chosen ciphertext attack and unforgeability against adaptive chosen message attack in random oracle model. Compared with two other Diffie-Hellman based signcryption schemes proposed by Barbosa and Farshim (BF) and another by Yin and Liang (YL), our scheme consumes 46 % and 8 % less energy during signcryption than BF and YL scheme respectively.