A new mutual authentication and key agreement protocol in wireless body area network

Title	A new mutual authentication and key agreement protocol in wireless body area network
Publication Type	Conference Paper
Year of Publication	2020
Authors	Wu, Xiaohe, Xu, Jianbo, Huang, Weihong, Jian, Wei
Conference Name	2020 IEEE International Conference on Smart Cloud (SmartCloud)
Date Published	Nov. 2020
Publisher	IEEE
ISBN Number	978-1-7281-6547-9
Keywords	anonymous messaging, authentication, Biomedical monitoring, body area networks, cryptography, key agreement, mutual authentication, Protocols, pubcrawl, resilience, Resiliency, security, WBAN, Wireless communication, Wireless sensor networks
Abstract	Due to the mobility and openness of wireless body area networks (WBANs), the security of WBAN has been questioned by people. The patient's physiological information in WBAN is sensitive and confidential, which requires full consideration of user anonymity, untraceability, and data privacy protection in key agreement. Aiming at the shortcomings of Li et al.'s protocol in terms of anonymity and session unlinkability, forward/backward confidentiality, etc., a new anonymous mutual authentication and key agreement protocol was proposed on the basis of the protocol. This scheme only uses XOR and the one-way hash operations, which not only reduces communication consumption but also ensures security, and realizes a truly lightweight anonymous mutual authentication and key agreement protocol.
URL	https://ieeexplore.ieee.org/document/9265963
DOI	10.1109/SmartCloud49737.2020.00045

Citation Key wu_new_2020

anonymous messaging authentication Biomedical monitoring body area networks Cryptography key agreement mutual authentication Protocols pubcrawl resilience Resiliency security WBAN Wireless communication wireless sensor networks