An enhanced Multi-Receiver Secure Data Transmission Protocol for WBANs

Yanwei Zhou, Zhaolong Wang, Zirui Qiao, Bo Yang, Wei Deng, Zhe Xia and Mingwu Zhang

TABLE I
ADVANTAGES AND DISADVANTAGES OF EXISTING SCHEMES

Scheme	Methods and Tools	Advantages	Disadvantages
Shen *et al.* [9]	* WBANs communication * Certificateless generalized signcryption * Performance simulation	* Avoids key escrow * Avoids certificates management * Multi-receiver data transmission	* Insecurity * High storage costs * High communication costs
Li *et al.* [20]	* WBANs communication * Bilinear mapping * Certificateless signcryption	* Confidentiality * Receiver anonymity * Privacy Protection	* High computational costs * Security proof based on non-static complexity assumptions * Only signcryption operations are supported
Noor *et al.*[21]	* WBANs communication * Certificateless signcryption	* Confidentiality * Receiver anonymity * Public verifiability	* Insecurity * Only signcryption operations are supported * Informal security proof
He *et al.* [28]	* ECC (Elliptic Curve Cryptography) * Certificateless encryption	* Multi-receiver encryption * Better computation efficiency	* Only encryption operation is supported * Huge communication and storage burden for users
Zhu *et al.*[29]	* Certificateless encryption * Bilinear map	* Multi-receiver encryption * Confidentiality	* Only encryption operation is supported * Informal security proof * High computation costs
Umrani *et al.*[30]	* Hybrid construction * Certificateless signcryption * ECC (Elliptic Curve Cryptography)	* Broadcast communication * Efficient transmission of large amounts of data	* Unreliable security proof * High communication costs * Only signcryption operation is supported
Yu *et al.* [31]	* Certificateless signcryption * ECC (Elliptic Curve Cryptography) * Implicit certificate	* Multi-receiver signcryption * Receiver anonymity	* Implicit certificates increase maintenance costs * Only signcryption operation is supported
Li *et al.* [32]	* Hybrid construction * Certificateless signcryption * ECC (Elliptic Curve Cryptography)	* Multi-receiver signcryption * Receiver anonymity	* Unreasonable signature verification * Only signcryption operation is supported * It can be affected by requiring the secure channel for the partial private key distribution
Tomar *et al.* [33]	* Certificateless signcryption * ECC (Elliptic Curve Cryptography) * Blockchain	* Data aggregation * Identity authentication	* The use of blockchain increases system maintenance costs * Only signcryption operation is supported * Verification parameter increase storage costs
Chenam *et al.* [34]	* Certificateless encryption * ECC (Elliptic Curve Cryptography) * Bilinear map	* Multi-receiver encryption * Supports keyword search	* High computation costs * Only encryption operation is supported * It will be affected by the lack of anonymity property
Chenam *et al.* [35]	* Certificateless encryption * ECC (Elliptic Curve Cryptography) * Standard model	* Multi-receiver encryption * Supports keyword search	* Unreliable security proof * Only encryption operation is supported * Suffering from a larger nature of bandwidth
Zhu *et al.* [36]	* Aggregate signcryption * Shamir's trick * Strong RSA assumption	* Data aggregation * Locally verifiable	* Key escrow problem * Only signcryption operation is supported * Private key distribution problem