Abstract

The application and usage of the wireless sensor network is rapidly growing. Wireless sensor networks are normally deployed into the unattended environment where the intended user can get access of the network. The sensor nodes collect data from this environment. If the data are valuable and confidential then some security measures are needed to protect the data from the unauthorized access. In this paper, I propose an identity-based user authentication and access control protocol based on the Identity-Based Signature (IBS) scheme where the ECC (Elliptic Curve Cryptography) based digital signature algorithm (DSA) is used for signing a message and verifying a message for a wireless sensor networks. This protocol accomplishes the registration of a new user, authentication of a user, session key establishment between sensor node and the user; and finally grants the appropriate data access to the user. User revocation is also handled in this proposed protocol. Compared with other conventional security solutions, this protocol provides confidentiality and integrity of the sensor data; and also achieves better computational, communicational performance and energy efficiency due to the use of more efficient IBS algorithms based on ECC than those based on RSA.

References

- Rehana Yasmin, Eike Ritter, and Guilin Wang (July 2010), An Authentication Framework
for Wireless Sensor Networks using Identity-Based Signatures, 10th International Conference on Computer and Information Technology (CIT).
- M. Choudary Gorantla, Colin Boyd, and Juan Manuel Gonzalez Nieto (2008), ID-based One-pass Authenticated Key Establishment, AISC.
- Wei Dai (September 2010), Crypto++ Library 5. 6. 1, Ibiblio-The Public’s Library and Digital Archive
- Erik Eliasson (May 2006), Secure Internet Telephony: Design, Implementation, and Performance Measurements, TRITA-ICT/ECS AVH 06:04
- Z. Benenson, F. Gartner and D. Kesdogan (2004), User authentication in sensor networks

Index Terms

Computer Science Wireless Security
Keywords
Wsn  Security  Authentication  Access Control  Ibs