Abstract

Smart Grid is a modern digital metering system that has been introduced to replace the traditional electricity infrastructure by collecting and utilizing information generated from different consumers automatically. Many researches have been conducted on the secure communication sessions to address the key issue of security in smart grid communication. Existing secure anonymous key distribution scheme for smart grid brings challenge such as key escrow problem in identity based encryption and identity based signature. In this paper we incorporate the first concept of certificateless in order to solve the key escrow problem that is found in identity based signature scheme and an identity based encryption scheme. Our proposed scheme achieves key escrow resilience which has not been achieved by previous work in this field.

References

1. Yan, Y., Qian, Y., Sharif, H. and Tipper, D. 2013 A Survey on Smart Grid Communication
Certificateless Secure Anonymous Key Distribution Scheme for Smart Grid

Infrastructures: Motivations, Requirements and Challenges, IEEE Comm. Smart Grid
6. Communications in smart distribution grid, IEEE Trans. Smart Grid
13. H. Krawczyk, 2005. HMQV: A high-performance secure DiffieHellman pro- tocol, in Proc. CRYPTO, Santa Barbara, CA, USA
15. Y. Wang, 2013. Efficient identity-based and authenticated key agreement protocol, in Transactions on Computational Science XVI. Berlin, Germany: Springer-Verlag
20. Recommendation for Key Management, Part 1: General,
Cryptol. (CRYPTO), Santa Barbara, CA, USA


29. M. Myers, R. Ankney, A. Malpani, S. Galperin, and C.


Index Terms

Computer Science
Security

Keywords

Certificateless, anonymity, Smart Grid, Smart Meters.