Abstract

In 1976, Diffie and Hellman in their path breaking paper [5] proposed a two party key agreement protocol based on finite field. Diffie–Hellman Key Exchange Protocol [DH protocol] has unique importance in two party wireless communication scenarios. After this protocol several protocols have been proposed bases on DH protocol but the Man in the middle attack raises a serious security concern on this protocol. Researchers have been working to overcome this security concern to design a new protocol. This paper proposes an authenticated key agreement protocol which is secure against Man in the middle attack. The authors also prove security issues of this protocol.

References


10. Menezes A., M. Qu, & S. Vanstone, Key agreement and the need for authentication, Proceedings of PKS'95, Toronto, Canada, 1995


Index Terms

Computer Science  Security
Keywords

Diffie – Hellman key agreement, Wireless Communication, Authenticated Key Agreement, Man in the Middle Attack (MITM), Security