Abstract

Wireless Sensor Networks (WSNs) with traditional cryptography are applied in many areas including healthcare, earth sensing and area monitoring. However, severe security constraints coupled with malicious attacks and threats revolve around the implementation of Wireless Sensor Networks which pose undesirable security performance as well as affect the maintenance of proper functionality of wireless sensor systems. Due to such circumstances, it is important to recognise the need for a holistic and robust security to ensure WSNs are well established and protected. In this study a more robust technique for a wireless sensor network system is employed. The algorithm for Elliptic Curve Diffie Hellman key exchange is studied and analyzed using PyCryptodome package and the Elliptic Curve Integrated Encryption Scheme. The study is carried out in comparison to Rivest-Shamir-Adleman (RSA) to assess the strengths of ECC in key generation and encryption/decryption process. The results obtained from the analysis reveals that ECC provides a higher level of security and also has very small key size in comparison to RSA, which makes possible implementations more compact for some level of security.
References


Index Terms

Computer Science Wireless

Keywords