Abstract

Communication security is one of the areas where research is highly required. The data used in communication is very sensitive and needs to be protected and made abstract from intruders of system. This research is all about securing the messages or data that is being communicated among two parties. The recent branch of Network security is Cryptography using Elliptic Curve Architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems. ECC schemes are public-key based mechanisms that provide encryption, digital signatures and key exchange algorithms. The best known encryption scheme is the Elliptic Curve Integrated Encryption Scheme (ECIES) which is included in IEEE and also in SECG SEC 1 standards. The key establishment protocol is Elliptic Curve MQV, with implicit certificates and symmetric key cryptographic techniques. The research focuses on achieving secrecy using ECIES algorithm for encryption, and authentication using Hashing technique. The hashed plaintext is again encrypted with RSA. At the receiver end, the hashed text is decrypted first. The hash value of the plaintext decrypted is compared with the latter hash. If they are found equal, the integrity can also be assured. The parameters to considered choosing Elliptic Curves are presented in NIST document of recommended elliptic curves.
References


Index Terms

Computer Science  Security

Keywords

Elliptic curve Cryptography  Integrated encryption scheme  information security
encryption-decryption scheme

security in Wireless sensor nodes (MANET's)

Message authentication