ABSTRACT

Security has become a primary concern to provide protected communication in wireless networks. Security features in wireless network systems depend on factors like small packet size, low bandwidth, low transmission costs, limited processing time, storage resources and real time constraints. A reliable and secure wireless communication can be achieved by providing confidentiality, authenticity, integrity, anonymity and availability.

Public-key cryptosystems offers robust solutions in securing wireless networks. The most widely used public-key cryptosystem is the Rivest-Shamir-Adelman (RSA) algorithm. RSA is based on integer factorization algorithm and hence factoring performance can be used as a benchmark against which the security of RSA can be evaluated. Attacks on RSA can be overcome by increasing the key size but this makes the key generation process more complex and time consuming. This also increases the time of the encryption and decryption algorithms, thereby increasing the storage requirement.

The drawbacks of RSA are overcome by Elliptic Curve Cryptography (ECC) which is emerging as an attractive public-key cryptosystem for wireless networks. It offers the highest security strength per bit of any known public-key cryptosystem. Moreover, the advantages of ECC are higher speeds, lower power consumption, bandwidth savings, storage efficiencies and smaller certificates. These advantages are particularly beneficial in applications where bandwidths, processing capacity, power availability and storage are constrained. Such applications include chip cards, electronic commerce, web servers, cellular telephones, sensor networks and pagers. The primary aim of this research work is to explore the performance advantages obtained by securing wireless networks using ECC in lieu of the traditional RSA.

ECC makes use of elliptic curves in which the variables and co-efficients are all restricted to elements of a finite field. ECC over elliptic curves are classified as ECC over prime fields and ECC over binary fields. To begin with, the performance advantages of ECC over prime fields were analyzed by implementing it in the
Handshake Protocol for Secure Sockets Layer (SSL). Generally SSL makes use of RSA scheme in its Handshake Protocol. The RSA operations performed in the Handshake Protocol of SSL is computationally expensive. Hence, the use of SSL with RSA imposes significant performance degradation in the web servers. However, integration of ECC in the Handshake Protocol of SSL leads to significant reduction in the computational cost of cryptographic operations. Performance improvement in terms of the simulation timing for the Handshake Protocol, Crypto Latency and Throughput were analyzed and presented.

ECC over binary field is more popular due to available space and time efficient implementation of Elliptic Curve arithmetic. Exploiting the advantages of ECC over binary fields, a mutual authentication and session key management protocol for Mobile Ad hoc Networks has been developed. The performance advantages of the developed protocol along with the simulated results are presented.

A high speed and less complex ECC algorithm over binary fields using a new Ring representation technique has been developed. The multiplication timing of ECC over binary fields has been reduced as the field elements in a Ring are defined by using simpler polynomials. This Ring representation in ECC over Fourth Term polynomial and Trinomial has been implemented and the simulated results were compared with the conventional Pentanomial in finite fields. The developed algorithm offers significant improvement in encryption/decryption timings.

Further, the developed high speed and less complex ECC algorithm over binary fields has been implemented for securing wireless sensor networks. The usage of the algorithm resulted in resolving the three main security issues viz., Localization, Time Synchronization and Routing with data reliability. Moreover, the developed high speed and less complex ECC algorithm has been integrated in the signature generation and verification process of ECDSA. This integration has resulted in significant improvement in signature generation and verification timings as against RSA and DSA. Subsequently, a hybrid certificate has been proposed using the developed algorithm. The proposed hybrid certificate offers improved certificate generation and verification timings.