The Internet and various other forms of electronic communication is such an essential thing to move up with this periodic global world and indulging security is another gradient to climb defeating those black hats. One essential aspect for secure communications is that of cryptography. In previous approaches RSA and ECC algorithms plays a vital role however both algorithms are lacking of mathematical problems monotonously. In our proposed approach a novel protocol called Shared Key Management (SKM) is employed. In this approach McElieec algorithm is embedded with Dispense Key designed for key generation and for the key distribution. This scheme is highly scalable with respect to memory moreover number of keys are drastically reduced. Experimental results are being encountered that our proposed approach increases its efficiency in terms of memory and execution time for performing both encryption and decryption. As a result this algorithm is providing a high-performance platform to execute key generation, key distribution encryption and decryption scenarios.

References
An Efficient SKM Framework for Data Authentication and its Application to the Adhoc Networks

- "A Summary of McEliece-Type Cryptosystems and Their Security" - D. Engelbert, R. Overbeck, and A. Schmidt, 2006
- "Attacking and defending the McEliece cryptosystem" - Daniel J. Bernstein, Tanja Lange, and Christiane Peters, Aug 2008
- "Elliptic Curve Cryptography" - An implementation Guide, Anoop MS, anoopms@tataelxsi.co.in
Index Terms

Computer Science  Wireless Security

Keywords

Skm Framework  Data Authentication  Adhoc Networks