LIST OF FIGURES

Figure **Page No.**

Figure 2.1: BiSNET Architecture 13

Figure 2.2: The Sensor Networks Protocol Stack 16

Figure 3.1: Elliptic Curve defined over Real Number 26

Figure 3.2: Addition of Points P & Q 27

Figure 3.3: Addition of Points P & -P 28

Figure 3.4: Doubling of Point P 29

Figure 3.5: Doubling of Point P if yP=0 30

Figure 4.1: Clustered Architecture of a WSN 49

Figure 6.1: Interaction between Classes of JCE/JCA 74

Figure 6.2: Software Architecture of ECDSA 74

Figure 6.3: Class Structure of ECDSA 75

Figure 6.4: Class Structure of RSA 76

Figure 6.5: Snapshot of 32-bit ECC based Proposed Scheme 78

Figure 6.6: Snapshot of Elliptic Curve Encryption Scheme 79

Figure 6.7: Snapshot 1 of 32-bit RSA based Encryption- Decryption Phase 80

Figure 6.8: Snapshot 2 of 32-bit RSA based Encryption- Decryption Phase 80

Figure 6.9: Snapshot 3 of 32-bit RSA based Encryption- Decryption Phase 81

Figure 6.10: Snapshot 4 of 32-bit RSA based Encryption- Decryption Phase 81

Figure 6.11: Snapshot of Characteristic Phase ECDSA from Proposed Scheme 82

Figure 6.12: Comparison of 163-bit ECC & 1024-bit RSA based Proposed Scheme 84

Figure 6.13: Performance Timings of 163-bit ECC based Proposed Scheme 85

Figure 6.14: Performance Timing of 1024-bit RSA based Proposed Scheme 86

Figure 6.15: Performance Timings of different n-bit ECC based Proposed Scheme 87

Figure 6.16: Comparison of n-bit ECC & 1024-bit RSA based Proposed Scheme 88

LIST OF TABLES

Table **Page No.**

Table 2.1: Characteristics of Smart Dust Sensors 17

Table 3.1: Illustration of computation of NAF(7) 45

Table 6.1: Comparison of Performance Timings of Proposed Scheme 83

LIST OF ALGORITHMS

Algorithm **Page No.**

Algorithm 3.1: Elliptic Curve Diffie-Hellman Protocol 39

Algorithm 3.2: Elliptic Curve Digital Signature Algorithm 41

Algorithm 3.3: Elliptic Curve Authentication Encryption Scheme 43

Algorithm 3.4: Computation of the NAF of scalar 44

Algorithm 3.5: Scalar Multiplication using the Addition-Subtraction method 46

Algorithm 3.6: Scalar Multiplication using Repeated Additions 47

Algorithm 4.1: Proposed Mutual Authentication & Key Mgt. Scheme for WSNs 59