Glossary

Glossary of terms used in the thesis are enlisted here.

**ActiS** Activity Sensor

**ADC** Analog to Digital Converter

**AES** Advance Encryption Standard

**AFECA** Adaptive Fidelity Energy Conserving Algorithm

**AKM** Authenticated Key Management

**AODV** Ad hoc On Demand Distance Vector Routing

**ASN** Ad hoc Sensor Network

**BECA** Basic Energy-Conserving Algorithm

**BFS** Byzantine-fault-tolerant NFS file system

**BIBD** Balanced Incomplete Block Design

**BROSK** Broadcast session key negotiation protocol

**BS** Base Station

**C4W** an identity-based PKI designed for WSN

**CA** Cellular Automata

**CAB** Cellular Automata Based key management

**CA** Certification Authority
CADR  Constrained Anisotropic Diffusion Routing

CBC  Cipher Block Chaining

CC  ChipCon

CCM  Counter with CBC-MAC

CDMA  Code Division Multiple Access

CEC  Cluster-based Energy Conservation protocol

CFB  Cipher Feedback Mode

CRT  Chinese Remainder Theorem

CSV  Comma Separated Value

CTMC  Continuous Time Markov Chain

CTS  Clear To Send

DARPA  Defense Advanced Research Projects Agency

DBSCAN  Density-Based Spatial Clustering of Applications with Noise

DC  Direct Current

DLP  Discrete Logarithm Problem

DMBS  Deterministic multiple space Blom’s scheme

DoS  Denial of Service

DSDV  Destination Sequenced Distance Vector Routing

DYMO  Dynamic MANET On Demand

EAR  Eavesdrop-And-Register

EBS  Exclusion-based system

ECC  Elliptic Curve Cryptography
**ECDH** Elliptic Curve Diffie Hellman

**ECDLP** Elliptic Curve Discrete Logarithm Problem

**ECDSA** Elliptic Curve Digital Signature Algorithm

**ECG** Electrocardiogram

**ECIES** Elliptic Curve Integrated Encryption Standard

**ECMQV** Elliptic Curve Menezes-Qu-Vanstone

**ECNR** Elliptic Curve Nyberg Rueppel

**ECPVS** Elliptic Curve Pintsov Vanstone Signatures

**EEG** Eelectro Encephalography

**EMG** Electromyography

**FPGA** Field-programmable Gate Array

**GAF** Geographical Adaptive Fidelity (GAF) algorithm

**GEAR** Geographical end Energy-Aware Routing

**GF** Galois Fields

**GPSR** Greedy Perimeter Stateless Routing for Wireless Networks

**GQ** Generalized Quadrangles

**HEED** Hybrid, Energy-Efficient, Distributed Clustering Approach

**HKD** Hint Key Distribution

**HKK** Hook Key

**HMAC** Hash-based Message Authentication Code

**HSR** Hierarchical State Routing

**HTTPS** HTTP over SSL or HTTP Secure
**HySecNJoining**  Hybrid Secure Node Joining

**IBE**  Identity Based Encryption

**IDS**  Intrusion Detection System

**IEEE**  Institute of Electrical and Electronics Engineers

**IMS**  IP Multimedia Subsystem

**IOS**  ID based one-way function scheme

**IP**  Internet Protocol

**IS**  Information System

**ISA**  International Society of Automation

**ISO**  International Organization for Standardization

**ISPM**  Intelligent Signal Processing Module

**ISSO**  Information System Security Officer

**KDC**  Key Distribution Centre

**KM**  Key Management

**LEACH**  Low-Energy Adaptive Clustering Hierarchy

**LEAP**  Lightweight Extensible Authentication Protocol

**LEAP**  Localized Encryption and Authentication Protocol

**LED**  Light Emitting Diode

**LOCK**  Localized combinatorial keying

**MAC**  Medium Access Control

**MAC**  Message Authentication Code

**MANET**  Mobile Ad hoc Network
MATLAB Matrix Laboratory
MAWSN mobile-agent-based WSN
MBS Multiple space Blom’s scheme
MCU Micro Controller Unit
MD Message Digest
MIC Message Integrity Code
MWE Multi-Winner Election
NDS Node Discovery
NFS Network File System
NIST National Institute of Standards and Technology
NS-2 Network Simulator 2
PDA Personal Digital Assistant
PDU Protocol Data Unit
PEGASIS Power-Efficient Gathering in Sensor Information Systems
PRF Pseudo Random Function
OAA Open Agent Architecture
OLSR Optimal Link State Routing
OPTICS Ordering Points To Identify the Clustering Structure
OSI Open Systems Interconnection
PDU Protocol Data Unit
PKC Public Key Cryptography
PKI Public Key Infrastructure
QoR  Quality of Routing
QoS  Quality of Service
RC2  Ron’s Code or Rivest’s Cipher 2
RF   Radio Frequency
RFC  Request For Comment
RFID Radio Frequency Identification
RSA  Rivest, Shamir and Adleman
RSN  Robust Security Network
RSNA Robust Security Network Association
RTS  Request To Send
SAR  Sequential Assignment Routing
SECK Survivable and Efficient Clustered Keying
SHA  Secure Hash Algorithm
SMACS Self Organizing Medium Access Control for Sensor Networks
SN   Sensor Node
SNEP Sensor Network Encryption Protocol
SOSUS Sound Surveillance System
SPAN Power Saving technique for multi hop Ad hoc Wireless Network
SPARC Scalable Processor Architecture
SPINS Security Protocols for Sensor Networks
SSH  Secure Shell
SSL  Secure Socket Layer
SSSL  simplified SSL

SQL  Structured Query Language

SWE  Single-Winner Election

TEEN  Threshold-sensitive Energy Efficient sensor Network protocol

TELOS  a family of motes from University of California Berkeley

TESLA  Timed, Efficient, Streaming, Loss-tolerant Authentication

TI  Texas Instruments

TLS  Transport Layer Security

TPM  Trusted Platform Module

TSSR  Two Stage Source Routing in sensor networks

USB  Universal Serial Bus

UWB  Ultra Wide Band

VPN  Virtual Private Network

WBAN  Wireless Body Area Network

WEP  Wired Equivalent Privacy

WINS  Wireless Integrated Network Sensors

WLAN  Wireless Local Area Network

WMN  Wireless Mesh Network

WPAN  Wireless Personal Areas Network

WSN  Wireless Sensor Network

XOR  Exclusive OR

XTEA  eXtended Tiny Encryption Algorithm