INDEX

Advanced Encryption Standard (AES), 23
ANODR, 106–109
Anomaly based detection, 156–158
Anonymous Routing protocols, 105–113
AODV, 72–73
Applications of wireless ad hoc networks, 5–6
Approximate point in triangle, 198
Ariadne, 84–90
Asymmetric key cryptography, 16, 23
Attacks, 10–12, 19
Authenticated Routing for Ad hoc Networks (ARAN), 77–79
Authentication, 16
Availability, 16
Biometrics, 16
Block ciphers, 21
Blom’s scheme, 62
Certification authority (CA), 41
Clustering, 140–144, 175–176
Common Information Model (CIM), 177
Common Open Policy Service (COPS), 176–177
Computation, 187, 199
Condition Action Rules, 166
Confidentiality, 16
Cooperative vehicular infrastructure system, 226
Data Encryption Standard (DES), 22
Dedicated short range communication, 225, 226
Denial of Service, 11
Deontic Logic, 165, 169
Destination-Sequenced Distance Vector (DSDV) routing protocol, 91
Deterministic key distribution schemes, 50
Diffie–Hellman, 26
Distance bounding, 204
Distance vector routing protocols, 69–70
Distributed Management Task Force (DMTF), 176–177
Dynamic Source Routing (DSR) protocol, 80–81
ECHO, 205
EndairA, 90–91
Event Condition Action Rule, 166–167
Firewall Management, 180–181
Fully distributed authority, 47
Global positioning system, 190
Global system for telematics, 226
Hash chains, 35
Hashed random preloaded subsets, 58
Hierarchical IDS, 138–140
Hierarchical policy management architecture, 171, 173–175
High-resolution range independent localization, 211
Hop-count based localization, 197
Host Intrusion Detection System (HIDS), 122–124
Insider nodes, 10
Integrity, 16
Intrusion Detection System (IDS), 120–159
IP Security Policy (IPSP), 177
Ismene Policy Description Language, 168–169
Key Distribution Centers, 41
KeyNote Trust Management System, 178–180
Lightweight Directory Access Protocol (LDAP), 177
Link state routing protocols, 69–70
Localized encryption and authentication protocol, 53
Location based key management, 65
Locators, 188

MASK, 109–113
Maximum likelihood, 200
Mesh networks, 6
Message Authentication Digests, 29
Message digests, 16, 27
Misuse detection, 158
Mobile Ad hoc Networks (MANET), 4–6
Modes of operation, 30
Multipath key reinforcement scheme, 56, 57
Multipoint Relays (MPRs), 99–101

Network Intrusion Detection System (NIDS), 122–124
Network on wheels, 226
Non-repudiation, 16

Optimized Link State Routing (OLSR) protocol, 99–101
Outsider nodes, 10

Packet dropping attack, 12, 151–155
Partially distributed authority, 45
Path key establishment, 54, 55
Peer Intermediaries for Key Establishment (PIKE), 63
Peer-to-peer IDS, 136–138
Peer-to-peer policy management architecture, 171–173
Policy Based Network Management (PBNM), 162–164, 177
Policy Conflict Resolution, 176.
Policy Decision Point (PDP), 163–164, 176–177
Policy Description Language (PDL), 169–170
Policy Enforcement Point (PEP), 163–164, 176–177, 181–183
Policy language, 165–170
Policy Management, 160–184
Ponder Policy Language, 167–168
Pre-image resistance, 27
Proactive routing protocols, 70–71
Probabilistic key distribution schemes, 50, 54
Product ciphers, 22
Promiscuous monitoring, 149–150

Q-composite scheme, 56
Random pairwise key scheme, 56, 58
Range dependent localization, 190
Range independent localization, 196
Ranging, 187, 189
Reactive routing protocols, 70–71
Received signal strength technique, 194
Rei policy language, 169
Reputation Schemes, 144–147
Robust position estimation, 220
Role Based Access Control (RBAC), 178
Routing attack, 10, 11–12, 155–159
RSA algorithm, 25
Rushing attack, 12, 117–118

S-DSDV, 98–99
Secure AODV, 73–77
Secure Efficient Distance Vector (SEAD) routing, 92–95
Secure Hash Algorithm (SHA), 28
Secure Link State Routing Protocol (SLSP), 103–105
Secure network encryption protocol, 52
Secure range independent localization, 211
Secure Routing Protocol (SRP), 81–84
Security aware Ad hoc Routing (SAR), 79–80
Self-Issued certificates, 47
Shared key-discovery, 54
Specification based detection, 158
Steganography, 16
Stream ciphers, 21
Strong collision resistance, 27
STRONGMAN, 179–180
Substitution cipher, 21
SuperSEAD, 95–98
Sybil attack, 11, 118–119
Symmetric key cryptography, 16, 20

TESLA, 35
Threats, 8
Threshold cryptography, 45
Time of flight technique, 192
Traffic analysis attack, 11
Transmission range variation scheme, 216
Transposition cipher, 21
Triangulation, 200
Trilateration, 200
Trusted third party, 40
Trust Management, 178–180
Vehicular ad hoc network, 225
Vehicular infrastructure integration, 226
Verifiable multilateration, 208
Vulnerabilities, 9

Weak collision resistance, 27
Wireless Ad Hoc networks, 4–6
Wormhole attack, 12, 113–117
X.509 certificate, 43