

Index

- 3G-SGSN 37
- A5 algorithm 32
- A8 algorithm 32
- access control 13
- access points (APs) 18–19
 - malicious 24, 44
- acknowledgement (ACK) packet 20
- active attacks on networks 43, 49–50
- active path sets (APSs) 144
- ad hoc BSS 18
- ad hoc Jini-based services 70–1
- ad hoc networks 1–3
 - compared with conventional systems 1
 - operating principles 3–7
 - QoS 14–15
 - security requirements 11–14
 - vulnerabilities 8–10
- ad hoc on demand distance vector (AODV) routing
 - protocol 91–2, 111, 131, 132, 133–4
- advanced encryption standard (AES) 28–9, 165–9
- anomaly detection 87
 - mobile wireless networks 94–6
- anonymity 13
- asymmetric digital signatures 10
- authentication 21, 22–3
- authentication center (AUC) 30–1
- authentication schemes 76
 - authentication, authorization and accounting (AAA) 79
 - end-to-end data authentication scheme 77–9
 - MANET authentication architecture 76–7
 - WiMax networks 160
 - vulnerabilities 169–70
- authenticity 11
- authorization 12
- authorization key (AK) 159, 162–3
- availability 11
- availability attacks 56

- base station controller (BSC) 31
- base station system (BSS) 30–1
- base transceiver station (BTS) 31

- basic service sets (BSSs) 18–19, 21
- battery power 7
 - DoS attacks 10
- beaconing 4
- billing center 37
- black hole attacks 51
- Bluetooth 2
 - security 40–1
- broadband wireless access (BWA) 147
- Byzantine failures 44, 84
- Byzantine robustness 13

- carrier sense multiple access with collision
 - avoidance (CSMA/CA) 20
- carrier sense multiple access with collision detection (CSMA/CD) 20
- cellular networks *see* wireless cellular networks
- certification authority (CA) 63
- circuit switched (CS) domain 35, 36
- clear-to-send (CTS) packet 7, 20
- cluster-based routing protocol (CBRP) 77
- confidentiality 11, 21
- cryptography 10
 - certification authority (CA) 63
- cryptosystems 13
- currency concept 137–41

- data aggregation attacks 47
- data forwarding 9
- decision-making 101
- denial-of-service (DoS) 9, 44–5
- destination-sequenced distance vector (DSDV) 111
- direct sequence spread spectrum (DSSS) 83
- distributed asynchronous key management service
 - 62–5
- distributed denial of service attack 45
- distribution system (DS) 18–19
- dynamic source routing (DSR) 94, 111

- eavesdropping 8, 43, 84
- effectiveness of IDSs 88
- efficiency of IDSs 88
- electromagnetic analysis attacks 59

- encrypted key exchange (EKE) protocol 66
- encryption
 - advanced encryption standard (AES) 165–9
 - MAC enhancements 27–9
 - UTRAN 40
- end-to-end data authentication scheme 77–9
- enterprise networks 27
- equipment identity register (EIR) 30–1
- Ethernet 18
 - compared with IEEE 802.11 networks 20
- exposed terminal problem 6
- extended service set (ESS) 18–19
- extendable authentication protocol (EAP) 25–6, 160–2
- external attacks on networks 44, 50–2

- fabrication attacks 49
- fair resource allocation attacks 47
- fault injection attacks 58
- firewalls 37
- flow-based route access control (FRAC) 92–3
- frequency hopped spread spectrum (FHSS) 83
- functional security mechanisms 53

- gateway GPRS support node (GGSNs) 32–4, 37
- gateway mobile services switching center (GMSC) 31
- General Packet Radio Service (GPRS) networks 32–3
 - subscriber authentication 33–4
- global system for mobile (GSM) networks 29–31
 - security 31–2
- Global Positioning System (GPS) 4, 111
- GPRS support nodes (GSNs) 32
- GSM interworking unit (GIWU) 31

- hardware, stolen 23
- hashed message authentication code (HMAC) 159
- hidden terminal problem 6, 20
- home location register (HLR) 30–1, 32
- HomeRF Shared Wireless Access Protocol 2
- host monitoring 101

- IEEE 802.11 networks 17–20, 29
 - compared with Ethernet 20
- IEEE 802.15 networks 40–1
- impersonation 45–6
 - Sybil attacks 46–7
 - Trust attacks 48
- independent BSS 18
- infrastructure BSS 18
- initialization vector (IV) 21
- integrity 11
- integrity attacks 55, 58
- interception attacks 49
- internal attacks on networks 44, 49–50
- Internet 3
- interruption attacks 49
- intrusion detection and response model (IDRM) 91
- intrusion detection systems (IDSs) 82–4, 102–5
 - MANETs 89–90
 - anomaly detection 94–6
 - AODV protocol-based system 91–2
 - distributed system 90–1
 - TIARA 92–3, 103, 104
 - watchdog-pathrater approach 93–4
- mobile agents 96
 - architecture based on static stationary database 98–100
 - distributed system 100–2
 - LIDS 96–8
 - overview 86–8
 - intrusion response 88
 - requirements 88–9
- IP networking 3
- isolation 12
- Iu interface 36

- jamming 45
- Jini 70

- key creation 13
- key distribution 13, 21
- key encryption keys (KEKs) 159
- key management 13, 62
 - distributed asynchronous key management service 62–5
 - minimal public-key-based authentication 68–9
 - non-disclosure method (NDM) 69–70
 - password-authenticated key exchange protocol 65–6
 - progressive trust negotiation scheme (NTM) 66–8
 - robust membership management scheme 72–5
 - robust ubiquitous security scheme 71–2
 - scalable ubiquitous security scheme 75–6
 - securing ad-hoc Jini-based services 70–1
- key storage 13

- lightweight computations 12
- line-of-sight (LOS) operation 148, 151
- link-state 114
- local area networks (LANs) 17
- local intrusion detection system (LIDS) 96–8
- location disclosure attacks 51–2
- location privacy 12
- logical link control (LLC) 18, 34
- loop-free paths 6

- MAL packet 92
- malicious access points 24, 44
- management information bases (MIBs) 97, 98
- MANET authentication architecture (MAA) 8
- masquerading node 133
- medium access control (MAC) 3, 6
 - BSS 18–19
 - encryption enhancements 27–9
 - WEP 21, 22
 - stolen hardware 23
 - WiMax networks 151–3
- message center (MXE) 31
- minimal public-key-based authentication 68–9
- misbehaviour detection attacks 47
- misuse detection 87
- mobile ad hoc network (MANET) routing protocols 8

- mobile computing 2
- mobile service node (MSN) 31
- mobile stations (MSs) 19–20, 30–1
- mobile switching center (MSC) 30–1
- modification attacks 49

- network interface card (NIC) 18
- network monitoring 101
- network switching system (NSS) 30–1
- node hijacking 52
 - secure ad hoc nodes 55–9
 - tamper-proof and -resistant nodes 53–4
- nodes 4–5
 - compromised 8–9
 - free roaming 9
 - scalability 10
 - trusted/non-trusted 9
 - dynamic allocation 10
- node-state 114
- non-disclosure method (NDM) 69–70
- non-line-of-sight (NLOS) operation 148, 149
- non-repudiation 11–12

- operation and control system (OSS) 31
- ordering 12

- packet charging gateway 37
- packet purse model (PPM) 138–40
- packet trade model (PTM) 139–40
- passive attacks on networks 43, 49
- password-authenticated key exchange protocol 65–6
- personal area networks (PANS) 17
- physical attacks 56, 57–8
- Piconet 2
- point-to-multipoint (PMP) topology 149, 153–5
 - bandwidth request header 154, 155
 - type encodings 154
- point-to-point (P2P) topology 149
- power analysis attacks 58
- pre-cursor attacks 59
- privacy 21
- privacy and key management (PKM) control 157
- privacy attacks 55, 59
- private keys 10
- progressive trust negotiation scheme (NTM) 66–8
- protocol date unit (PDU) 152
- PURGE packet 92

- quality of service (QoS) 2, 6, 14–15, 107–10, 126–7
 - routing 110–12
 - routing with QoS constraints 112–18
 - ad hoc networks 118–25
 - WiMax networks 156–7
- radio network controller (RNC) 35
- radio network subsystem (RNS) 35
- RADIUS server 25–6
- random challenge (RAND) 32
- REMA packet 92
- request-to-send (RTS) packet 7, 20

- resource release message 121
- resurrecting duckling 61–2
- Rijndael algorithm 28–9
- Rivest, Ronald 21
- robust membership management scheme 72–5
- robust ubiquitous security scheme 71–2
- Ron's Cipher-4 21
- route failure message 121
- route-reply (RREP) message 131, 132
- route-request (RREQ) message 131, 132
- routing 110–12, 129
 - mitigating routing misbehaviour 136–7
 - QoS constraints 112–18
 - ad hoc networks 118–25
 - secure message transmission protocol (SMTP) 141, 143–5
 - secure packet forwarding (currency concept) 137–41
 - secure routing protocol (SRP) 141–3
 - security aware routing (SAR) 129–31
 - operation 132
 - protocol 131–2
 - route discovery in SAODV 132–3
 - security distant-vector routing protocols 133–6
 - summary of security features 145
- routing attacks 47
- routing message protection 135
- routing table overflow attacks 51
- routing update protection 135–6

- scalability of networks 10
- scalable ubiquitous security scheme 75–6
- secure routing protocol (SRP) 141–3
- security 17, 41
 - see also* Worldwide Interoperability for Microwave Access (WiMax) network security
 - see also under* routing
 - Bluetooth 40–1
 - vulnerabilities in MANETs 84–6
 - wireless cellular networks
 - GPRS 32–4
 - GSM 29–32
 - Universal Mobile Telecommunications System (UMTS) 34–40
 - WLAN networks 17–20, 29
 - authentication and privacy 21
 - dealing with threats 24–7
 - MAC encryption enhancements 27–9
 - medium access 20
 - native security schemes 21–3
 - threats 23–4
- security association (SA) 157–9
- security association identity (SAID) 157–8
- self-stabilization 12
- sensor networks 10
- service data unit (SDU) 152
- service set identifiers (SSIDs) 21–2
- servicing GPRS support node (SGSNs) 33–4
 - 3G-37
- side-channel attacks 56, 57–9

- signed response (SRES) 31–2
- simple network management protocol (SNMP) 97
- sleep deprivation attacks 51
- SMS-GMSC 37
- software attacks 56, 57
- specification based detection 87–8
- stolen hardware 23
- subscriber authentication 33–4
- subscriber identity module (SIM) 31–2
- subversion attacks 49
- subverted links 134
- subverted node 134
- Sybil attacks 46
 - direct communication 46
 - examples 47
 - fabricated or stolen identities 46
 - indirect communication 46
 - non-simultaneous 47
 - simultaneous 47
- SYN flooding 45

- tamper-proof and -resistant nodes 52–4
- techniques for intrusion-resistant ad hoc routing
 - algorithms (TIARA) 92–3, 103, 104
- temporal key integrity protocol (TKIP) 28
- temporary mobile station (TMSI) 34
- threats and attacks 23–4, 43
 - attack classification 43–4
 - disclosure 48–9
 - DoS 44–5
 - impersonation 45–6
 - Sybil attacks 46–7
 - Trust attacks 48
 - in-transit information 49
 - node hijacking 52
 - secure ad hoc nodes 55–9
 - tamper-proof and -resistant nodes 53–4
 - routing or network layer 49
 - external attacks 50–2
 - internal attacks 49–50
- threshold cryptography 64
- timeliness 12
- time-out mechanism 121–2
- timing analysis attacks 58
- topology discovery 9
- topology of networks 1, 4–6
- traffic encryption keys (TEKs) 158, 163–4
- transport-layer security (TLS) 70
- trust 13–14
- Trust attacks 48
- trust management 61, 79–80
 - authentication 76
 - authentication, authorization and accounting (AAA) 79
 - end-to-end data authentication scheme 77–9
 - MANET authentication architecture 76–7
 - key management 62
 - distributed asynchronous key management service 62–5
 - minimal public-key-based authentication 68–9
 - non-disclosure method (NDM) 69–70
 - password-authenticated key exchange protocol 65–6
 - progressive trust negotiation scheme (NTM) 66–8
 - robust membership management scheme 72–5
 - robust ubiquitous security scheme 71–2
 - scalable ubiquitous security scheme 75–6
 - securing ad-hoc Jini-based services 70–1
 - resurrecting doorking 61–2
- trust model 13

- UMTS terrestrial radio access network (UTRAN) 35
 - encryption 40
- unauthorized node 134
- Universal Mobile Telecommunications System (UMTS) networks 34–6
 - CS domain 36
 - mutual authentication 38–40
 - packet-switched domain 37–8
 - UTRAN encryption 40

- virtual private network (VPN) 21
 - security 26–7
- visitor location register (VLR) 30–1
- voting attacks 47
- vulnerability of mobile ad hoc networks 84–6

- watchdog-pathrater 93–4, 136–7
- wide area networks (WANs) 17
- wired equivalent privacy (WEP) 21, 22
 - stolen hardware 23
- wireless cellular networks
 - security 41
 - GPRS 32–4
 - GSM 29–32
 - Universal Mobile Telecommunications System (UMTS) 34–40
- Wireless Ethernet Compatibility Alliance (WEPA) 22
- wireless local area networks (WLANs)
 - security 17–20, 29
 - authentication and privacy 21
 - dealing with threats 24–7
 - MAC encryption enhancements 27–9
 - medium access 20
 - native security schemes 21–3
 - threats 23–4
- wireless mobile networks 1
- wireless security *see* security
- Worldwide Interoperability for Microwave Access (WiMax) network security 147–8, 171
- frame structure
 - MAC layer 151–3
 - physical layer 151
- mesh 155–6
- open issues 169
 - authentication vulnerabilities 169–70
 - key management 170

180

Worldwide Interoperability (cont.)
PMP mode 153–5
QoS 156–7
security features 157
 authentication 160
 data encryption 164–9
 extensible authentication protocol 160–2
 privacy and key management 162–4
 security associations 157–9

Index

 standardization and certification 148
 frequencies 148–9
 modes of operation 149–50
wormhole attacks 52

X.509 certification 160
 fields 162

zone routing protocol (ZRP) 111