

INDEX

- Access control, 360
- Access points (APs)
 - building, 34
 - campus WLAN studies, 17–19, 32–40
 - client-side tools, 15–16
 - loss, 14–15
 - malfunctioning, 6, 25
 - management information bases (MIBs), 11
 - mapping, 16, 24
 - network sniffing, 13
 - nonacademic WLANs, 20–21
 - personal digital assistants (PDAs), 18
 - quality of service (QoS), implications of, 47, 53
 - single-queue comparisons, 58, 63
 - SNMP community, 16, 25
 - syslog messages, 6–9, 16, 25
 - usage studies, 24, 30
 - VoIP, single queue, 61
 - wireless sniffing, 14–15
- Acknowledgment (ACK) packet
 - MANETs, 77
 - VoIP, 49, 56, 61, 63–64, 66
- Acknowledgment spoofing, 299
- ACM SIGCOMM, 20
- ACS log, 34–36
- Ad hoc networks, security issues, 284.
 - See also* Mobile ad hoc networks (MANETs)
- Ad hoc on-demand distance vector (AODV) protocol, multihop wireless networks, 107–109, 125, 127, 129–131, 134–135
- Adaptation algorithms, 47
- Adaptive House (University of Colorado-Boulder), 338
- ADDTs request, 55
- Adjusted best-point heuristic, 235
- Admission control
 - contention-based, 48, 54–55, 70
 - quality of service (QoS) provisioning, 47–48, 58
- Admission control mandatory (ACM) subfield, 54
- AES encryption, 286, 290, 303
- Aggregate-commit-prove, 300
- Aggregation, wireless sensor networks, 299–302
- Aging problem, storage management, 271–272
- AIFS, quality of service (QoS), 46–47
- All-pair shortest-path algorithm (APSP), 232
- All-sensor field intensity, 231
- Altered routing information, 299
- Always-on devices, 24
- Ambient noise, 120
- Annealing, simulated, 247
- Announcement traffic indication message (ATIM), MANETs, 97–98
- Anomaly detection, 297
- Anonymization, 33
- Antenna, *see specific types of antennae*
 - functions of, 15, 197
 - MANETs, 83
 - power control design and, 77
- Apple Airport, 31
- Art gallery problem (AGP), 224, 238

- Assistive environments, 342
- Association
 - campus WLAN studies, 19
 - syslog messages, 9
 - wireless-side measurement studies, 21
- Asymptotic equipartition property, 349–350
- Atheros, 14
- Attacks. *See also* Hackers
 - denial-of-service, 223, 286–287, 364
 - event fabrication, 301
 - insider, 364
 - link layer, 288
 - malicious mobile node flooding, 363–364, 370, 375, 378
 - man-in-the-middle, 360, 373
 - redirect, 360, 362–364, 369, 378
 - sinkhole, 299
 - Sybil, 288, 299
 - traffic permutation, 369–370
 - on wireless sensor networks, 287–289
- Attenuation, field gathering wireless sensor networks, 212
- Attractive forces, wireless sensor networks, 241
- Audio/video (AV) streaming, quality considerations, 45
- Augmented reality applications, storage management, 260, 279
- Authentication
 - campus WLAN usage studies
 - implications of, 18, 31, 36
 - LEAP, 32
 - home binding, 361–362, 366, 368, 372–373, 376
 - logs, 11–12, 17, 30, 32
 - mobile target tracking, 192
 - mutual entity, 360
 - protocols, 223
 - security issues, 287
 - wireless sensor networks, 289–291
- Backoff algorithms, 46
- Backoff process, 48–49
- Bandwidth
 - allocation, MANETs, 80
 - coherence, 99
 - on demand, 397–398
 - sensor networks, 176–177, 180
- Barrier coverage, 224
- Basestation
 - placement of, 2
 - security issues, 290, 292, 299
 - wireless sensor networks, 222
- Battery/batteries
 - capacity, 109
 - level, 78
 - power, wireless sensor networks, 221, 261
 - replacement, 292
- Battlefield monitoring/surveillance, 191, 197, 223
- Bayes' rule, 150, 152
- Beacon(s)
 - intervals, MANETs, 96–97
 - wireless sensor networks, 285
- Belief state, mobile target tracking
 - 182–183
- Bellman–Ford shortest path algorithm, 82, 115, 208
- Best-point heuristic, 235
- Bidding protocol (BIDP), 243–244, 248
- Billing, metered, 397
- Binary hypothesis testing, wireless sensor networks, 145–146, 149–152, 154
- Binary phase shift keying (BPSK), 120
- Binary sensing model, 225–226
- Binary sensors, 174, 177–180
- Bit error rate (BER), 92, 119–120, 126–129, 136
- Blanket coverage, 224
- Bluetooth, 343
- Bootstrapping protocol, 292, 296
- Bottlenecks, sources of, 91, 109, 213, 216, 278
- Boundary conditions, 233, 240
- Breadth-first search (BFS), 236
- Broadband
 - defined, 392
 - managed services, 381–382
 - sensor networks, 191–194
- Broadcast ID, multihop wireless networks, 129, 131–134
- Broadcast incremental power (BIP)
 - algorithm, 83
- Broadcast storm problem, 80
- Building-access point relation, 34
- Building maps, 16, 24
- Business flexibility, 387
- Busy-tone channel, MANETs, 87–88

- Campus waypoint, 18
- Campus wireless network usage
 - methodologies
 - analysis, 33–34
 - anonymization, 33
 - authentication logs, 32
 - trace collection, 32–33
 - network environment, 31–32
 - overview of, 29–30, 42–43
 - related work, 30–31
 - results
 - ACS log, 34–36
 - roaming patterns, 36–40
 - trace data, 40–42
- Campus WLANs, 16–20
- Candidate routes, 3
- Capital expenditures (CapEx), 399–400, 403
- Carrier sense multiple access with collision avoidance (CSMA/CA), 45, 48, 75, 83
- CBC-MAC, 290
- Cellular networks, 2
- Cellular phones, 105, 372, 389–392
- Cellular systems, power control design, 84, 86, 91
- Center of stimulus (CoS), 301
- Certification authority (CA), 365, 374
- Channel
 - access
 - controlled, 51
 - DCF, 49
 - EDCA, 51–52
 - quality of service (QoS), 47
 - conditions, VoIP, 58
 - error rates, multihop wireless networks, 122
 - load, quality of service (QoS), 47
 - utilization measurement, 48
- Cisco
 - Aironet 350, 6–7, 31
 - AP1200 access points, 31
 - AP350 access points, 31
 - Internetworking Operating System (IOS), 6, 8
 - LEAP (Lightweight Extensible Authentication Protocol), 18, 31–32
 - probe response studies, 22
 - Secure ACS, 32
- Clear-to-send (CTS) packet
 - MANETs, 75, 81, 83, 87–90, 93–94, 96–97
 - multihop wireless networks, 127
- Client-side tools
 - campus WLAN studies, 18
 - characteristics of, 24
 - WLAN measurement, 15–16
- Cluster-based collaborative storage (CBCS)
 - components of, 265–270
 - security issues, 286
- Cluster-based communication model, 296
- Cluster head (CH)
 - characteristics of, 91
 - cluster-based collaborative storage, 266
 - election phase, cluster-based collaborative storage, 266, 286
 - intrusion detection, 298
 - key management, 293, 296–297
 - security issues, 302
- Clustering
 - field gathering wireless sensor network, 211–213, 216
 - MANETs, 90–91
 - wireless sensor networks, 146, 253
- Cluster rotation, 266–267
- CMMBCR algorithm, 109
- Coherence bandwidth, 99
- Coherence time (T_c), 90
- Collaboration model, wireless sensor network, 216
- Collaborative signal and information processing (CSIP), 222
- Collaborative storage
 - benefits of, 264
 - coordinated sensor management, 266–267
 - design space, 265
 - experimental evaluation, 267–271
 - multiresolution-based storage, 271–273
 - protocols, 265–266
- Collectors, wireless sensor networks, 198, 205–208, 212
- Collision(s)
 - avoidance information, 87, 89, 99
 - MANETs, 76, 95
 - mobile target tracking, 194
 - VoIP, 68, 70
- COM+, 320
- Combinatorial optimization, 252

- Communication graph, 228
- Communication model, 226
- Compression, 55. *See also* Data compression
- Concurrent transmissions, 76, 86
- Conditional probability, 246
- Confidentiality, 286–287, 290
- Configuration grid, 244–245
- Connected environments, 341
- Connected network, 225
- Connected topology, mobile target tracking, 187
- Connectivity
 - global network, 251
 - graph, field gathering wireless sensor networks, 215
 - influential factors, 77
 - MANETs, 82
 - sensor networks, 143
 - wireless sensor networks, 228–229, 295
- Connectivity-based clusters, 266
- Connectivity set (CS), MANETs, 89
- Constant-bit-rate (CBR), 56
- Contention window (CW), 49
- Context-aware smart environment, 346
- Continuous density function, 204–205
- Controller nodes, 295
- Control packet overhead, mobile target tracking, 194
- Convex hulls, binary sensor network tracking, 177–178
- Convoy tree, mobile target tracking
 - characterized, 185
 - construction of, 186
 - expansion and pruning, 186
 - reconfiguration, 186–187
- Cookies, 367–369, 374–375
- Cooperative tracking, binary detection
 - sensor networks, 179–180
- Coordinated collaborative storage (CCS), 267–269
- Coordinated local storage (CLS), 267–270
- Coordinated sensor management, 266–267
- Coordinators, MANETs, 98
- CoralReef
 - analysis package, 34
 - toolset, 40
- CORBA, 309, 320
- Cordless telephones, 95
- Corrupt data packets, 222
- Cougar, 271
- Covering coding, 188
- Critical transmission range (CTR)
 - assignment, 229
- Crossing point, 249
- Cross-layering, 74
- Cryptographically generation address (CGA)
 - protocol, 361, 371–372, 378
- Cumulative energy, 106
- Current interference, MANETs, 84
- CW_{min} , 46–47
- Cyber pet caring game, 395
- Damagochi, 395
- Dartmouth College, campus WLAN usage studies, 18–19, 30–31
- Data
 - access patterns, 259
 - acquisition, 283
 - analysis software, testing of, 25
 - collection
 - methodologies, 5–6
 - sensor networks, 259–262, 283
 - Simple Network Management Protocol (SNMP), 11
 - software, testing of, 25
 - wireless sensor networks, 283
 - compression
 - storage management, 267
 - universal, 348
 - wireless sensor networks, 205–208, 214
 - corruption, detection of, 263
 - exchange phase, cluster-based
 - collaborative storage, 266
 - freshness, 289
 - gathering, wireless sensor networks, 252–253
 - generation, rate of, 258–259
 - manipulation costs, 258
 - processing, wireless sensor networks, 159
 - retention, 262
 - transmission, wireless sensor networks, 159–160
- Data-centric storage (DCS), 271, 274–275, 277
- DCF interframe space (DIFS), 48–49, 52, 56
- DCOM, 309, 320
- Deauthenticate events, syslog messages, 9
- Deauthentication, campus WLAN usage studies, 31

- Decentralized algorithms, 216
- Decision rules, 147, 151–154, 168–170
- Decryption, 294, 299
- Degree of coverage, sensor networks, 224–225, 229, 240
- Delaunay triangulation, 237
- Delay
 - AODV, 135
 - MANETs, 95
 - propagation, 90
 - VoIP, 60–61
 - wireless sensor networks, 122–123
- Denial-of-service (DoS) attacks, 223, 286–287, 364
- Deployment probability distribution, 204
- DES, 290
- Destination node, 198
- Device control, 340–341
- DHCP servers, access to, 16, 40
- DHCPv6, 361
- Diffie–Hellman key exchange algorithm, 374–376, 379
- Digital signature, 286, 365, 373
- Dijkstra algorithm, 115, 232, 234
- Directed diffusion, 271
- Directional antennas (DAs), 2, 93–95, 99, 209, 299
- Directional network allocation vector (DNAV), 94
- Directory Name Service (DNS), 372
- Direct subscriber line (DSL), 383–384
- Disassociation, 9–10, 19
- Disk space, 13, 25
- Distance mapping, mobile target tracking (MTT), 181–182
- Distributed coordination function (DCF)
 - characterized, 1
 - interframe space, 48–49, 52, 56
 - legacy, 48–49, 58
 - quality of service (QoS)
 - channel access, 52
 - comparative performance evaluation, 56, 63
 - defined, 45
 - dual-queue scheme, 51
 - legacy, 53
 - modification of, 46
- Distributed data compression, 206
- Distributed hash table (DHT) system, 274
- Distributed index for features in sensor networks (DIFS)
 - architecture, 278–279
 - high-level event, 278
 - overview of, 277–278
 - simple quad tree approach, 278
- Distributed self-spreading algorithm (DSSA), 241–242, 247
- Distributed tracking schemes, mobile target tracking (MTT)
 - group management for track initiation, 182–184, 191
 - maintenance, 182, 184–185
 - tracking tree management, 185–187
- Diurnal usage patterns, campus WLAN studies, 17–19
- Doppler spread, 90
- Drilldown constraints, in storage management, 273
- Dual busy-tone multiple access (DBTMA), MANETs, 88
- Dual-queue scheme
 - implications of, 49–50
 - legacy DCF, 48
 - MDQ, 45–46
 - VoIP, 68
- Dynamic adjustment scheme, 47
- Dynamic convoy tree-based collaboration (DCTC), 185–186
- Dynamic source routing (DSR)
 - MANETs, 79, 91
 - multihop wireless networks, 107, 109, 125
- Eavesdropping, 222, 289, 373
- E-commerce, 382
- Edinvar Assisted Interactive Dwelling House, 338
- Effective bit energy-to-noise spectral density ratio, 92
- Effective reliable throughput, 121
- Embedded software, 395
- Enclosure graph, 82
- Encryption
 - algorithms, 223
 - implications of, 13
 - mobile target tracking, 192
 - wireless sensor networks, 286, 289–291, 294–295, 299

- End-to-end
 - communication, 389
 - enabling IT infrastructure, 386
 - packet delivery, MANETs, 78, 80
 - reliability, 106
 - retransmission (EER), multihop wireless networks
 - assigning link costs, 115–118
 - characterized, 107–108
 - on-demand routing protocols, 130, 132–134
 - optimal minimum-energy paths, 110–115
 - performance evaluation, 118, 121, 123–125
 - systems, 395
- Energy-aware (EA) routing, 105, 118, 122, 135
- Energy conservation, 252–253
- Energy-constrained nodes, 249
- Energy consumption
 - MANETs, 78–79
 - storage management, 261
 - wireless sensor networks, 158–161, 223, 250, 297
- Energy cost analysis, 109–115
- Energy-efficient
 - communication, 2
 - networks, MANETs, 78, 92–93
 - protocol stack, 82
 - routing, multihop wireless networks, 114
- Enhanced distributed channel access functions (EDCAFs), 53
- Enhanced distributed channel access (EDCA)
 - characteristics of, 2
 - comparisons with
 - default access vs. PIFS access, 66–68, 70
 - MDQ, 63–66
 - quality of service (QoS), *see* Enhanced distributed channel access (EDCA)
 - quality of service
 - parameter set, 53
- Enhanced distributed channel access (EDCA) quality of service (QoS)
 - characterized, 45–46
 - comparative performance evaluation, VoIP
 - access, default vs. PIFS, 66–68, 70
 - characterized, 56–57
 - MDQ, 63–66
 - defined, 51
 - 802.11e provisions, 51–54
 - transmission opportunity (TXOP), 51, 54
- Enterprise service bus (ESB), 388, 390
- Entropy coding, 207–208, 214
- Environmental conditions, 259
- Environmental hazard monitoring, 197, 221, 224, 289
- Error-free delivery, 3
- Error rate, multihop wireless networks, 109–110. *See also* Bit error rate (BER); Link error rate
- Ethernet, 12–14, 325, 360
- EtherPeek, 18, 32
- Euclidean distance, 225, 240
- Euler–Lagrange equation, 233
- Event correlation, 397
- Event fabrication attacks, 301
- Execution phase, 245
- Expected average ability, 230
- Exposure paths
 - implications of, 251–253
 - maximal
 - best-case-coverage, 230, 234–235
 - breach path, worst-case coverage, 230, 235–237
 - support path, best-case coverage, 230, 237
 - minimal, worst-case coverage, 230–234
- Extensible Markup Language (XML), 319, 326–329, 331, 388, 396–397
- Fabrication technologies, 173
- Fading, multihop wireless networks, 106
- Farfield propagation, field gathering wireless sensor network, 210
- Fast-backoff scheme, 47
- Fault tolerance
 - sensor collaboration, 175, 180
 - wireless sensor networks, 194
- FDMA, 95
- Feedback channel, MANETs, 84
- FFS, 263
- Fidelity, 31, 98, 138, 173, 382, 404–405
- Field gathering wireless sensor network
 - characteristics of, 142

- data compression, 205–208, 210, 214
- defined, 198
- fluid flow model, 201
- implications of, 197–199
- lifetime limits, energy constraints
 - data compression, 205–208
 - defined, 198–199, 216
 - mathematical framework, 200–204
 - model and assumptions, 199–200
 - network layout and, 204–205
 - throughput tradeoff, 216
- open problems, 215–216
- throughput limits
 - data compression, 214
 - defined, 198, 208–210
 - many-to-one communication results, 209–210, 212–214
 - model and assumptions, 210–211
 - one-on-one communication results, 211–212
 - practical algorithms, 214–215
- Field intensity, 231
- File-sharing, 19
- Filesystem limits, 13
- Firewalls, 25
- Firmware
 - changes, 25
 - 802.11 card, 15
 - upgrades, 6
- First-in/first-out (FIFO) transmission queue, 48, 58
- First-order derivatives, 233
- Fixed power level, 75
- Fixed-transmission power, 128
- Flash memory, storage management, 261–264
- Flat architecture, 216
- Flood-fill algorithm, 245
- Flooding, 223
- Flow
 - augmentation, 78, 202
 - fluid, 201
 - redirection, 202
 - traffic, 252
 - TCP, 56
 - unidirectional, 56
- Fluid flow model, 201
- Forward-error correction codes, 106
- Forward progress rate, 77
- Frequency
 - channels, CDMA-based MANETs, 96
 - reuse distance, 91
- FTP/TCP, unidirectional flow, 56
- Functional lifetime, 201
- Gain, MANETs, 85, 93
- Gateways, MANETs, 91
- Gaussian distribution, 246
- Gaussian noise, 146
- Generic loss, 14
- Geographic adaptive fidelity (GAF) MANETs, 98
 - multihop wireless networks, 138
- Geographically-based clusters, 266
- Geographic hash table (GHT) system, storage management:
 - canonical methods, 275
 - characteristics of, 274–276, 279
 - distributed index for features in sensor networks (DIFS), 277–279
 - interaction with greedy perimeter stateless routing (GPSR), 276
 - perimeter refresh protocol, 276–277
 - structured replication, 277
- Geometric fidelity, 173
- Geometric random graph (GRG), sensor network coverage, 227–228
- Georgia Tech
 - Aware Home, 338
 - wireless LANs, 17
- Global networks
 - on-demand, 389
 - topology, mobile target tracking, 185
- Global positioning system (GPS), 16, 24, 82
- Global signaling channel, 83
- GLOBUS, 309
- Gloucester Smart Home, 338
- Goal resolution phase, 245
- Goal selection phase, 244–245
- Gossiping, 223
- Graph EMbedding (GEM) for sensor networks, 277
- Graphical user interface (GUI), 393
- Graphs, sensor networks
 - characterized, 224–225
 - graph-theoretic perspective
 - geometric random graph (GRG), 227–228
 - graph connectivity, 228–229

- Greedy perimeter stateless routing (GPSR), 276–277, 299
- Grid
 - deployment, mobile target tracking, 192–193
 - network, wireless sensor network, 251
 - topology, multihop wireless networks, 136–137
- Group(s), mobile target tracking (MTT)
 - formation, 183
 - management strategies, 183–184
- G.711, defined, 55
- Hackers, 360, 364, 404
- Handheld computers, 32
- Handheld devices, 93
- Handshake packets, 75, 87
- Hardware abstraction layer (HAL), 395
- Hash value, 364
- HCF controlled channel access (HCCA), 51
- Health monitoring, 283
- Hierarchical architecture, 216
- Hierarchical sensor networks, 191–194
- Hierarchical summarization, 272
- High-mobile users, campus WLAN usage studies, 20, 31
- Histograms, quad trees, 278
- Home
 - binding update, 361–362
 - location, 19
 - node, geographic hash table (GHT) system, 276–277
- Home agent proxy (HAP), 361–362, 372–379
- Homeland defense, 283
- HomeRf wireless networking system, 95
- Hop-by-hop retransmission (HHR),
 - multihop wireless networks
 - assigning link costs, 115–116
 - characterized, 107–108, 137
 - on-demand routing protocols, 132–134
 - optimal minimum-energy paths, 114–115
 - performance evaluation, 118, 121–123
- Hops, *see specific types of hops*
 - energy-efficient reliable packet delivery, 105–106
 - number of, 3
 - transmission range and, 76–77
- Hostile environment, 191
- Hostnames, 16
- Hotspots, 1, 5, 46, 277, 382, 404
- HTTP, 17, 40, 42, 325, 328
- Hub and spoke infrastructure, 396
- Human-machine interface (HMI), 395
- Human-subject research, 13, 24
- Hybrid coordination function (HCF):
 - defined, 45, 50
 - IEEE 802.11e standards, quality of service (QoS), 50–51
- IBM, 386, 393, 395, 400
- ICQ, 17
- Idle listening, 192, 194
- Idle power consumption, 286
- IEEE 802.11 standards:
 - access points (APs), 6, 8, 53
 - authentication, 12
 - deauthentication, 12
 - infrastructure network, 6, 8–9
 - MAC layer, 14, 21–22, 45, 49, 268
 - management information base (MIB), 10
 - network interface cards (NICs), 10, 14–15, 22
 - PHY/MAC layer, 14, 21–22, 45, 49
 - power control, 74–76, 95
 - power saving modes (PSM), 96–99
 - QoS provisioning, 45–70
 - smart environments, 343
 - syslog message, 6, 9
 - VoIP, 58
 - wireless sniffing, 14
- IEEE 802.11b standard, 99
- IEEE 802.11e
 - admission control, contention-based, 48, 54–55
 - enhanced distributed channel access (EDCA), 48, 51–54
 - implications of, 2, 50–51
 - quality of service (QoS), 46
- IEEE 802.15.4 standard, 304
- IEEE 802.2, 55
- IETF Mobile IP Working Group, 361, 365–366
- Imprecise detections algorithms (IDA), 238–239, 247
- Incremental self-deployment algorithm (ISDA), 244–245, 248
- Index node selection, 279

- Industrial, Scientific, and Medical (ISM):
 - radio band, 2.4-GHz, 95
 - wireless sensor network, 343
- Industrial sensing, 141
- Information-driven sensor network tracking, 175–177
- Information processing, sensor networks, 277
- Information technology (IT)
 - functions of, 384
 - simplification, 387
- Information Technology Services Division (ITS), 30, 32–33
- Initialization phase, 244
- In-network processing, 303
- “Insider” attacks, 364
- Inspection, MANETs, 84
- Institutional review boards, functions of, 13, 24
- Insufficient reasoning, 349
- Integer linear programming algorithm (ILPA), 244, 246, 248
- Integrity, security issues, 287
- Intelligent control, 354
- “Intelligent” routing protocol, 78
- Intel Proactive Health Project, 338
- Intended receiver, MANETs, 87
- Interface identifier, 371
- Interference
 - field gathering wireless sensor networks, 210–211, 215
 - MANETs, 76–77, 86–87, 89
 - margin, MANETs, 87, 89
- Interference-aware protocol, MANETs, 84–91, 99
- Interframe space (IFS), 46
- Intersil Prism, 14
- Intrusion detection system (IDS), 197, 284, 297–298
- Inventory management, 197
- IP address, 16, 360, 372–373
- IP protocols, campus wireless networks, 40–41
- IP telephony, *see* Voice over IP (VoIP)
- IRC, 17
- ISM (Industrial, Science, and Medical)
 - wireless networking, 343
- Isotropic antenna, 94
- Jamming, 287–288
- Java virtual machine (JVM), 395
- Jitter, VoIP, 68–70
- k*
 - connectivity, 225
 - edge connectivity, 229
 - neighbors, 239–240
 - node-connected, 225
 - sensors, 253
- Kerberos authentication logs, 17
- Keyed pseudorandom function, 365
- Key exchange algorithm, 374–379
- Key management, security issues, 287, 292–297
- Key predistribution scheme (KPS), 289, 295–296
- Kids Communicator (AT&T), 342
- Laptops, 19, 93, 105, 384, 389
- Large attenuation, 212
- Large-scale sensor networks, 249
- Large-scale wireless sniffing, 24
- Latency
 - cooperative mobile target tracking, 180
 - wireless sensor networks, 223, 252
- Layer 4–7 switching, 402–403, 405
- LEACH, 268, 299
- Leader-based mobile target tracking, 182–184
- Legacy DCF, 48–49, 58
- Lempel–Ziv (LZ), 347
- Lexicographic max-min node lifetime
 - problem, 204
- LeZi-update scheme, MavHome, 347–349
- Likelihood ratio, 150, 177
- Linear programming, wireless sensor networks lifetime, 201–205
- Link error rate
 - implications of, 2
 - multihop wireless networks
 - characteristics of, 107, 112, 114, 117
 - estimation of, 126–129, 135
- Link layer attacks, 288
- Link-layer quality indicator (LQI), 47–48
- Link loss rates, 106
- Link scheduling, 109
- Load-aware routing, field gathering wireless sensor networks, 213

- Load balancing, storage management, 270
- Loading, MANETs, 96
- Lobe interference, MANETs, 94, 99
- Local area network, 37
- Localized encryption and authentication protocol (LEAP), 18, 31–32, 296
- Local storage (LS), 267–270
- Login, remote, 12
- Log-structured file system, 263–264
- Long-distance hops, 106, 112
- Long-range hops, 107
- Loss recovery, multihop wireless networks, 117–118
- Low attenuation, 212
- Lucent NIC, 22

- Malicious mobile node flooding attacks, 363–364, 370, 375, 378
- MALITDA, 338–339
- Management information base (MIB), 10
- “Manager of managers,” 393
- Man-in-the-middle attack, 360, 373
- Many-to-many communication, field
 - gathering wireless sensor networks, 209–210, 212–214
- Mapping
 - access points (APs), 16, 24
 - campus wireless roaming studies, 39–40
 - graph connectivity, 229
- Markov chain, applications of, 17–18
- Markov predictors, campus WLAN studies, 20
- M*-ary FSK (frequency shift keying), 120
- Matchbox file system, 258, 263–264
- Mathematical framework
 - communication model, 143, 226
 - coverage model, 226–227
 - sensing model, 225–226
- MavHome (University of Texas—Arlington):
 - architecture, 344–345
 - automated
 - decisionmaking, 351
 - inhabitant action prediction, 350–351
 - inhabitant location prediction, 346–350
 - characteristics of, 310, 338, 344–345
 - funding resource, 339
 - goal of, 351
 - implementation, 351–354
 - live demonstration of, 353
 - trie, 349
 - zones, 347–348
- Maximum permissible range, 116
- Maximum segment size (MSS), 56
- Maximum weight matching, 95
- Measurement tools
 - authentication logs, 11–12
 - client-side tools, 15–16
 - network sniffing, 12–13
 - SNMP, 10–11
 - syslog, 6–10
 - wireless sniffing, 14–15
- Medical equipment, 95
- Medium access control (MAC)
 - campus WLAN usage studies, 32
 - channel access parameters, 46
 - characterized, 2, 45
 - 802.11e provisions, 51–52
 - HW queue, 50, 60, 63–64
 - interference-aware, 84–90, 99
 - legacy, 48–49, 51
 - MANETs, 82–91, 99
 - network sniffing, 12
 - security issues, 288, 301–302
- Service Access Point (SAP), 55
- Simple Network Management Protocol (SNMP), 10–11
 - storage management protocols, 267
 - syslog messages, 8–10, 24
 - transmission range and, 77
- VoIP, 55–56
- Mesh networks, 406–407
- Message authentication code (MAC), 367–368
- Metadata, storage management, 263
- MICA, 284, 302–303
- MICA nodes, 262
- MICA-2, 262–263
- MICA2DOT, 262
- Microelectromechanical sensors (MEMs)
 - functions of, 221, 405
 - microsensors, 141
- Microsoft MSN Messenger, 55
- Microwave ovens, 95
- Middleware
 - architecture, 309
 - categories of, 319
 - computer-network-related, 309
 - defined, 316

- functions of, 318–319
- IT infrastructure, 318, 388–389
- MavHome, 310
- on-demand business, 310–311, 387–388
- RFID, 309, 313–325, 332
- security issues, 310
- support for sensor networks, 309
- technologies, 316–319
- web services, 319–320
- WinRFID, 309, 313, 323–324, 328–331
- Military applications
 - security issues and, 283, 294
 - sensor networks, 141
 - target tracking, 191–192
 - wireless sensor networks, 197, 221, 224, 260
- Minimal cutset, 298
- Minimax algorithm, 242–243, 248
- Minimum-description-length principle, 350
- Minimum energy consumed per packet
 - routes, 95
- Minimum-hop path, wireless sensor
 - networks, 202
- Minimum-hop routing algorithm, 118, 121
- Minimum-hop routing protocol (MHRP), 78, 80, 89–90, 105–106, 121, 181
- Minimum transmission power, MANETs, 84–85
- MIPS R4000, 286
- MIPv4, 361
- MIPv6, security issues
 - authenticating binding update messages
 - cryptographically generated addresses (CGA) protocol, 361, 371–372, 378
 - home agent proxy (HAP) protocol, 361–362, 372–379
 - implications of, 365–366
 - return routability (RR), 361, 366–371, 378
 - cryptographic primitives, 364–365
 - future directions, 378–379
 - importance of, 310
 - location privacy, 379
 - operations, 361–362
 - public key infrastructure (PKI), 376–379
 - redirect attacks, 360, 362–364, 369, 378
- Mirrored traffic, 32–33
- Mixed-sensor networks, 243, 248, 251–253
- MMBCR algorithm, 109
- Mobile ad hoc networks (MANETs)
 - CDMA-based, 95–96, 100
 - characterized, 2, 73–74
 - power control design
 - complementary approaches, 91–96
 - energy-oriented approaches, 77–82
 - IEEE 802.11 deficiencies, 75–76
 - power saving modes (PSM), 96–98
 - standard characteristics, 73–75, 98–100
 - TPC, MAC perspective, 82–91
 - transmission range, 76–77
- Mobile IP (MIP), 360–361
- Mobile IP Working Group, 368
- Mobile networks, security enforcement,
 - importance of, 359–361. *See also* MIPv6, security issues
- Mobile sensor networks, 238, 243–244, 247–248, 252
- Mobile target tracking (MTT), using sensor
 - networks
 - distributed tracking
 - network architecture design, 174, 187–194
 - protocol support for, 174, 182–187
 - implications of, 142, 173–174
 - information-driven dynamic sensor
 - collaboration, 175–177
 - multiple target tracking, 182
 - power-efficient, 174–175, 179–180, 194–195
 - quality of surveillance, 189–191
 - robustness, 175
 - target localization methods
 - using binary sensors, 174, 177–180
 - sensor-specific methods, 180–182
 - track initiation and maintenance, 182–185
 - traditional, 174–177
 - warning messages, 181–182
- Mobility
 - campus WLAN studies, 19–20
 - power control and, 90
 - traces/tracing, 16–18, 24
- Modified dual queue (MDQ), quality of
 - service (QoS)
 - characterized, 50, 58
 - comparative performance evaluation, 56, 61–66, 68–69
 - comparison with
 - EDCA, 63–66, 70
 - single queue, 58–63

- Motorola MC68328, 286
- Movement adjustment scheme, 243–244
- Moving objects, tracking with binary sensor network, 177–178
- MP3 music download service, 394
- Multiaccess interference (MAI), 95
- Multihop(s)
 - ad hoc networks, routing algorithm, 107
 - communication, security issues, 284
 - field gathering wireless sensor network, 213
 - path, transmission range and, 77
 - RTS, 94
 - security issues, 294
 - sensor networks, 222–223
 - wireless networks, *see* Multihop wireless networks
- Multihop wireless networks, energy efficient
 - reliable packet delivery
 - characteristics of, 107–108
 - on-demand routing protocols
 - adaptations for, 125–135
 - extensions for, 135–137
 - related work, 108–109
 - routing algorithms, minimum energy paths
 - assigning link costs, 115–118
 - energy cost analysis, 109–115
 - overview, 105–107, 137–138
 - performance evaluation, 118–125
 - roadmap, 108
- Multimodality, 389
- Multipath key reinforcement scheme, 295–296
- Multiple access interference, MANETs, 91
- Multiple tracking, mobile target tracking, 184
- Multiplicative increase, multiplicative/linear decrease (MIMLD) algorithm, 47
- Multiresolution-based storage
 - aging problem, 272–273
 - constraints, 273
 - drilldown queries, 272
 - overview of, 271–272
 - summarization, 272
- Multisensor systems, 173
- Multivendor networks, 304
- µTESLA, 290–291
- Mutual entity authentication, 360
- Near-far problem, 95, 100
- Neighbor/neighborhood
 - discovery, 362
 - field gathering wireless sensor network, 208
 - list, 132
 - MANETs, 84, 87–88, 96
 - multihop wireless networks, 118
 - one-hop, 276
 - security issues, 292
 - Voronoi, 235
 - wireless sensor networks, 240, 250, 285
- .NET, 330–331
- NetBSD kernel, 33
- Net hop, 78
- Network analysis, campus WLAN usage studies, 32
- Network architecture, mobile target tracking
 - broadband sensor networks, 191–194
 - deployment optimization, 188
 - hierarchical sensor networks, 191–194
 - power conservation, 188–191
- Network congestion, limitation strategies, 47–48
- Network disruption, minimization of, 25
- Network environments, significance of, 31–32
- Network interface card (NIC), 10, 14–15, 22, 50
- Network layers, MANETs, 82
- Network partitions, 78
- Network sniffing, 12–13, 17
- Network sysadmin, 13
- Network throughput, 209
- Network topology, 33, 57
- Network transport capacity, 209
- Node density, 222
- Node placement, sensor networks, 143
- Node redundancy, 223
- Node scheduling schemes, 252
- Node-to-node communication, 223
- Noise
 - ambient, 120
 - field gathering wireless sensor networks, 210
 - multihop wireless networks, 135–136
 - spectral density, 119
 - wireless sensor networks, 146
- Nonacademic WLANs, 20–21

- Non-real-time (NRT) queues, 49–50, 61, 63
- Normalized energy, 120–121
- Ns-2 simulator, 118, 267
- Occupancy maps, wireless sensor networks, 244–245
- Omnidirectional antennas, 93–94, 210
- On-demand business
 - application aware, 397
 - defined, 383
 - end systems, 394
 - evolution of, 386, 391
 - flowchart, 394
 - hardware abstraction layer (HAL), 395
 - implementation of, 388–389
 - mesh networks, 406–307
 - network layering, standardization
 - considerations, 402–404
 - operating environment, 384–394
 - OSS/BSS layers, 399–401
 - overview of, 310–311, 401, 407–408
 - pervasive computing ecosystem, 394–395
 - sensor networks, 405–407
 - service-oriented architecture (SOA)
 - defined, 387
 - principles of, 395–396
 - service access domains, 396–399
 - service domains, 399–401
 - wireless security, 404–405
- On-demand power-aware routing protocol, 79
- On-demand routing protocols, multihop wireless networks
 - adaptations for, 125–135
 - extensions for, 135–137
- One-hop
 - clustering algorithm, 266
 - neighbors, 250, 276
- One-on-one communication, 211–212
- One-way hash function, 364
- Operation expenditures (OpEx), 399–400, 403
- Optimal geographic density control (OGDC), 249
- Optimal node density, 251
- Optimal quantization algorithm, 153–154, 156–157, 159
- Oracle RDBMS, 327
- Orinoco (Lucent), 14, 22
- Oscillation control scheme, 243
- OSPF, 106
- OSS/BSS networking, 399–401
- Overhearing, 192, 194
- Overprovisioning networks, 387
- Packet(s)
 - collision effect, 58
 - drop rate, VoIP, 58
 - energy-efficient delivery, 2
 - error rate, multihop wireless networks, 120, 127
 - header(s)
 - analysis, 34
 - campus WLAN usage studies, 33
 - characteristics of, 13, 30–31
 - loss rate, 1, 3
 - sniffing, 12–13
 - traces, 13
 - transmissions, multihop wireless networks, 110–112
- Packetization, VoIP, 55
- Palm OS, 32
- Pareto distribution, 20
- Parsing, syslog messages, 8–9
- Partitioning, 93, 259–260
- Pebbles, defined, 293
- Peer-to-peer caching systems, 31
- Peer-to-peer (P2P) networks
 - characteristics of, 406
 - security issues, 286
 - storage management, 273–274, 279
- PEGASIS, 299
- Perl modules, 11
- Per node throughput, 209
- Per node transport capacity, 209
- Personal digital assistants (PDAs), 18–19, 105, 330, 372, 392
- Phoneline networking alliance (PNA), 343
- Physical layer (PHY)
 - characterized, 45
 - field gathering wireless sensor network, 210
 - quality of service (QoS)
 - implications of, 49
 - VoIP admission control, 56
- PHY/MAC layer, 21, 49
- Playback analysis, 259–260
- Plug-and-play technology, 392

- Point coordination function (PCF), 48, 51
- Point-to-point wireless links, long-range, 32
- Poisson process, 20
- Poll-and-response mechanism, 48
- Port mirroring, 12
- Position verification, 289
- Postenergy, defined, 268
- Potential field algorithm (PFA), 239–240, 247
- Power amplification, 92, 210
- Power-aware multiaccess protocol with signaling (PAMAS), 97, 106, 108
- Power-aware routing (PAR), 74
- Power-aware routing optimization (PARO), 79–80, 106, 108, 111
- Power-aware routing protocols (PARPs), MANETs, 78–81, 99
- Power consumption, 78, 223
- Power control design, mobile ad hoc networks (MANETs)
 - complementary approaches, 91–96
 - energy-oriented, 77–82
 - IEEE 802.11 approach, deficiencies of, 74–76, 95
 - overview of, 73–75, 98–100
 - power-saving modes, 96–98
 - transmission power control (TPC), 82–91
 - transmission range, selection factors, 76–77
- Power-controlled dual channel (PCDC), MANETs, 85, 88–90
- Power-controlled MAC protocols, 2
- Power-controlled multiple access (PCMA), 87–88
- Power failures, 31
- Powerline control systems, 340, 343
- Power-save polls, wireless-side measurement studies, 22
- Power saving modes (PSM), 2, 10, 74, 96–99
- Prediction by partial match (PPM), 349–350
- Prediction models, campus WLAN studies, 20
- Predictive caching systems, 31
- Preenergy, defined, 268
- Prepare mode, mobile target tracking, 190–191
- Primitives, public-key-algorithm-based, 284
- Priority access parameters, 55
- Prism NIC, 22
- Privacy, 13
- Proactive routing protocols, 78–79, 82, 107
- Proactive wakeup (PW) algorithm, mobile target tracking, 190–191
- Probabilistic sensing model, 226–227
- Probability distribution function (PDF), sensor network connectivity, 228
- Probe(s)
 - messages, MANETs, 97
 - multihop wireless sensor networks, 126–128, 135–136
 - response polls, wireless-side measurement studies, 22
- Processors, 197
- Propagation
 - delay, 90
 - field gathering wireless sensor network, 210, 212
 - multihop wireless networks, 106
 - wireless sensor network model, 215–216
- Protocol model, field gathering wireless sensor networks, 211, 213
- Pseudo-random-noise (PN) code, 95
- Public key certificate, 365, 373, 376
- Public key exchange, 374–378, 379
- Public key infrastructure (PKI), 376–379
- Pulse-coded modulation (PCM), 55
- PVM, 309
- QAP, 54–55, 66, 69
- q*-Composite random key predistribution scheme, 295–296
- Q*-learning, 351
- QoS STA (QSTA), 52, 54–55, 66
- Quad trees, storage management, 278
- Quality of service (QoS)
 - MANETs, 97
 - on-demand business, 398
 - significance of, 1–2
 - positioning, *see* Quality of Service (QOS), IEEE 802.11 WLAN
 - power control design, 77
 - wireless sensor networks, 222–223
- Quality of Service (QOS) positioning, IEEE 802.11 WLAN
 - channel access parameters, 46–47
 - comparative performance evaluation characterized, 56–57

- comparison of MDQ and EDCA, 63–66
 - EDCA default access vs. PIFS access, 66–68, 70
 - jitter performance comparison, 68–70
 - single queue and MDQ, 58–63
 - VoIP capacity for admission control, 56, 58
- dual-queue scheme for, 49–50
- emerging IEEE 802.11e
 - admission control, contention-based, 54–55
 - enhanced distributed channel access (EDCA), 51–54
 - implications of, 50–51
- legacy DCF, 48–49, 58
- overview of, 45–46
- related work, 46–48
- voice over IP (VoIP), for admission control
 - characterized, 55
 - 802.11b capacity for, 56
- Query/queries
 - drilldown, 272
 - execution, data collection, 259–262
 - overhead, 271
 - wireless sensor networks, 285
- Radio
 - resource testing, 289
 - transceiver, 197, 285
- Radiofrequency (Rf)
 - circuit design, 222
 - wireless sniffing, 14
- Radiofrequency identification (RFID)
 - applications of, 309, 313–314, 331–332
 - benefits of, 321–322
 - challenges of, 322–323
 - current technologies, 317
 - data processing layer, 326
 - ecosystem research at WINMEC, *see* WinRFID
 - implementation of, 320, 325
 - overview of, 314–315, 320
 - physical layer, 324–325
 - protocol layer, 325
 - tags, types of, 316, 325
 - web services, 320
- Radius, wireless sensor networks
 - of complete influence, 237
 - implications of generally, 226, 228
 - of no influence, 237
- Random pairwise key scheme, 295
- Random path heuristic, 234–235
- Range queries, 278
- Rate control, 2
- RC5, 290
- Reachability grid, wireless sensor networks, 245
- Reactive routes, MANETs, 77
- Real-time (RT)
 - queues, 49–50, 58, 64, 66
 - services, quality of service, 45–46
- Real Time Streaming Protocol (RTSP), 40, 42
- Reassociation, wireless-side measurement studies, 21
- Rebooting, automatic, 13
- Receiver, multihop wireless networks, 106
- Rectangular sensing field, 252
- RedHat Up2Date, 13
- Redirect attacks, 360, 362–364, 369, 378
- Redundancy, 174, 223, 249, 266, 288
- Reencryption, 294
- Refreshing, 276–277, 293
- Reinforcement learning, 351
- Relays, wireless sensor networks, 198
- Reliable communication, MANETs, 84–85
- Reliable delivery, multihop wireless networks, 111
- Reliable packet delivery, 106
- Remote access, 12
- Remote activated switch (RAS), 97
- Renegotiation, MANETs, 84–85
- Replayed routing information, 299
- Reprogramming, 285
- Repulsive forces, 241
- Request-to-send (RTS) packet
 - MANETs, 75, 81, 83, 87–88, 90, 93–94, 96–97
 - multihop wireless networks, 127
- Residual battery capacity, 109
- ResiSim update, 352–353
- Resource
 - consumption, mailbox file system, 264
 - management, wireless sensor networks, 253
 - testing, benefits of, 288–289

- Retransmission(s)
 - multihop wireless networks, 106–109, 111, 113–114, 117, 121–125, 137
 - potential, 2–3
- Retransmission-energy-aware (RA)
 - algorithm, 118, 122, 135, 136
- Return routability (RR), 361, 366–371, 378
- RFC 1812, 10
- RF spectrum, wireless sniffing, 14
- RIP, 106
- Roam events, syslog messages, 9
- Roaming patterns, 36–40
- Robotics, 337, 340, 342
- Robustness
 - geographic hash table (GHT) system and, 276
 - sensor collaboration, 175
 - sensor networks, 146, 166–170
- Rockwell WINS sensor nodes, 303
- Rogue packets, wireless sensor networks, 223
- Role assignment, field gathering wireless sensor networks, 203
- Roundtrip delay, multihop wireless networks, 122–123
- Route discovery process
 - MANETs, 79
 - multihop wireless networks, 132–135
- Routed networks, 32
- Route reply (RREP) packet
 - MANETs, 79–80, 88
 - multihop wireless networks, 129–135
- Route request (RREQ) packets
 - MANETs, 77, 79, 88–89, 91
 - multihop wireless networks, 129–135
- Routers
 - network sniffing process, 12
 - Simple Network Management Protocol (SNMP), 10
 - wireless sniffing, 15
- Routing
 - algorithm, 2
 - altered, 299
 - dynamic source, 79, 91, 107, 109, 125
 - energy-aware, 105, 118, 122, 135
 - energy-efficient, 114
 - greedy perimeter stateless, 276–277, 299
 - “intelligent,” 78
 - IPv6, 361
 - layer, 2
 - load-aware, 213
 - minimum-hop, 78, 80, 89–90, 105–107, 118, 121, 181
 - multihop networks, 105–125, 171
 - multipath, 299
 - power-aware, 74, 78–81, 99, 106, 108, 111
 - proactive protocols, 78–79, 82, 107
 - replayed information, 299
 - rumor, 299
 - shortest-path, 95, 176–177
 - wireless sensor networks, 146, 176–177, 223, 298–299
- RSA encryption, 286, 292
- RS-232, 325
- RS-485, 325
- RTP transport, 55
- RTS/CTS exchange
 - MANETs, 81, 83, 87, 90, 93, 97
 - multihop wireless networks, 127
- RTSP, 42
- Rumor routing, 299
- Scalar quantizers, 214
- Scheduling
 - of nodes, 249
 - phase, MANETs, 91
 - schemes, 249–250, 252
- Scientific data gathering, 197
- Scientific monitoring, 259–260, 271, 279
- Secondary routes, MANETs, 97–98
- Secure socket layer (SSL), 376–377, 379
- Security
 - authentication logs, 11–12
 - sensor networks, 143
 - Simple Network Management Protocol (SNMP), 11
 - surveillance, 221
 - wireless sensor networks
 - aggregation, 299–302
 - applications, 284–285
 - attacks, 287–289
 - data encryption/authentication, 289–291, 299
 - implementation, 302–304
 - intrusion detection, 284, 297–298
 - key management, 287, 289–297
 - overview of, 286–287
 - resources, 285–286

- routing, 298–299
 - significance of, 283–284
- Self-detection algorithm, 244
- Self-scheduling, 250
- Sensing field, intensity of, 232, 234
- Sensing gaps, 175
- Sensing model, 225–226
- Sensor deployment strategies
 - bidding protocol (BIDP), 243–244, 248
 - characterized, 238
 - comparison of, 246
 - distributed self-spreading algorithm (DSSA), 241–242, 247
 - imprecise detections algorithms (IDA), 238–239, 247
 - incremental self-deployment algorithm (ISDA), 244–245, 248
 - integer linear programming algorithm (ILPA), 244, 246, 248
 - minimax algorithm, 242–243, 248
 - potential field algorithm (PFA), 239–240, 247
 - security issues, 284–285
 - uncertainty-aware sensor deployment algorithm (UADA), 246, 248
 - vector-based algorithm (VEC), 242–243, 248
 - virtual force algorithm (VFA), 240–241, 247
 - Voronoi-based algorithm (VOR), 242–243, 248
- Sensor networks, wireless
 - applications, 382–383
 - centralized option, analysis of
 - characterized, 147, 149–151, 158, 160–161
 - detection performance, 170
 - numerical results, 163–164
 - robustness, 166, 168, 171
 - characterized, 145–148, 170–171, 221–223
 - connectivity, 221–253
 - coverage
 - based on exposure paths, 230–237
 - based on sensor deployment strategies, 238–248
 - future research directions, 252
 - mathematical framework, 225–229
 - types of, 221–224
 - detection performance, 146–147, 155–158, 164, 170
 - development of, 197
 - distributed option, analysis of
 - characterized, 147, 149, 151–153, 158, 160–161
 - detection performance, 170
 - numerical results, 163–164
 - robustness, 166, 168, 170–171
 - energy-efficiency analysis
 - energy consumption model, 158–161, 171
 - numerical results, 161–166
 - energy optimization, 146, 197
 - field gathering
 - implications of, 197–199
 - lifetime limits, 199–208, 216
 - open problems, 215–216
 - throughput limits, 208–216
 - mobile target tracking (MTT)
 - distributed tracking, protocol support for, 182–187
 - implications of, 173–174
 - network architecture design, 187–194
 - target localization methods, 174–182
 - multihop routing, 171
 - operating options, 149–150
 - protection of, 284
 - quantized option, analysis of
 - characterized, 147, 149, 163–164
 - optimal, 153–154, 156–157, 159
 - robustness, 166, 169
 - suboptimal, 154–157, 159–161
 - research, 141–143
 - robustness
 - implications of, 146, 171
 - node destruction, 166
 - observation data deletion, 167–170
 - routing algorithms, 146
 - security, 283–304
 - simplified model, 148–149
 - storage management, *see* Storage management for wireless sensor networks (WSNs)
- Service differentiation, quality of service (QoS), 46–47
- Service-level agreements (SLAs), 398–399

- Session
 - diameter, 19
 - hijacking, 363–364, 377–378
- SHA1 algorithm, 33
- SharePoint, 327
- Shortest-cost path, 117
- Shortest-delay (SD) AODV protocol, 135
- Shortest-path
 - algorithms
 - MANETs, 78–79, 82–83
 - routing, sensor network tracking, 176–177
 - heuristic, 235
 - routing, 95, 176–177
 - tree, 208
- Short hops, 106, 112
- Short IFS (SIFS), 49, 54
- Short-range hops, 107
- SIGCOMM, 21
- Signal processing, 221
- Signal strength, 10, 18, 78
- Signal-to-interference-and-noise ratio (SINR), MANETs, 76, 84, 86–87, 91
- Signal-to-noise ratio (SNR)
 - multihop wireless networks, 126–129, 137
 - wireless sensor networks, 158
- Signature (misuse) detection, 297–298.
 - See also* Digital signature
- Simple Network Management Protocol (SNMP)
 - campus WLAN studies, 18–19, 30–31, 40
 - wireless measurement, 10–11, 16–17, 24–25
- Simple Open Access Protocol (SOAP), 330
- SIMPLE, MANETs, 77–78, 99
- Simulation, wireless sensor networks, 252–253
- Simultaneous transmissions, field gathering wireless sensor networks, 212–214
- Single-beam directional antennas, 95
- Single-channel, signal transceiver distributed systems, 84
- Single-hop 802.11 deployment, 2
- Single queue, comparison with MDQ, 58–63
- Single-source shortest-path algorithm (SSSP), 232, 234
- Sinkhole attacks, 299
- Sink node, 198
- Skype, 393
- Sleep-awake-active pattern, 193
- Sleep mode, 254, 284
- Sleep period, mobile target tracking, 189–190
- Sleep-to-active transmission, MANETs, 97–99
- Slepian-Wolf model, field gathering wireless sensor network, 206–208
- Smart dust sensors, 222, 286, 405–406
- Smart environments
 - defined, 337
 - device communications, 338, 341
 - enhanced services by intelligent devices, 342
 - networking standards, 342–343
 - overview of, 337–340
 - predictive decisionmaking capabilities, 343–344
 - remote control of devices, 340–341
 - schematic view of, 338
 - sensory information acquisition/dissemination, 341–342
 - smart home illustration, *see* MavHome
 - types of, 337–338
- Smart sensor network, 180
- Smart Sofa, 342
- Snapshot, field gathering wireless sensor network, 198, 207–208, 214
- SNEP, 290, 303
- Sniffing
 - in measurement studies
 - network, 12–13
 - wireless, 14–15
 - nonacademic WLAN studies, 20
- Software, up-to-date, 13
- Software as a service (SaaS), 398–399
- Source-destination pairs
 - field gathering wireless sensor networks, 212, 215
 - MANETs, 79
 - multihop wireless network, 107–108, 110
- Sources, wireless sensor networks, 198
- SPAN
 - MANETs, 98
 - multihop wireless networks, 138
- Spatiotemporal data summarization, 271–272
- SPINS, 290–291, 293, 303
- Sponsor nodes, 250

- Spoofted routing information, 299
- Spread-spectrum technology, 2, 95
- SQL server, 327
- ssh usage, campus WLAN studies, 17–18, 21
- Stanford University, campus WLAN usage studies, 17, 31
- Static field gathering networks, 209
- Static sensor networks, 238–239, 243–244, 247–248, 252, 276, 285
- Station (STA), VoIP
 - dual-queue scheme, 51
 - ED default vs. PIFs access, 66–68, 70
- Stationary users, nonacademic WLAN studies, 20
- Station up/down messages, 8
- Statistical en route filtering (SEF), 301
- Storage constraints, 273
- Storage management for wireless sensor networks (WSNs)
 - collaborative
 - characterized, 257–258, 262, 264, 279
 - cluster-based (CBCS), 265–267
 - coordinated, 267–270
 - design space, 265
 - storage balancing effect, 270–271
 - storage-energy tradeoffs, 261, 268–270, 279
 - storage protocols, 265–266
 - components of, 262
 - data retrieval, 273–277, 279
 - design considerations, 257, 260–261
 - effective, 143, 260–261
 - efficiency of, 258
 - goals, 258, 261–262
 - indexing, 273, 277–279
 - load balancing, 278
 - motivation for, 259–260
 - significance of, 257–258, 279–280
 - system support
 - hardware, 262–263, 279
 - Matchbox file system, 258, 263–264
- Structured networks, storage management, 273
- Subdividing, field gathering wireless sensor network, 211–212
- Subnets
 - campus WLAN usage studies, 31–32
 - characterized, 25
 - wireless, 11–12
- Sub-Network Access Protocol (SNAP), 55
- Suboptimal minimum connected sensor covers, 252
- Suboptimal quantization algorithm, 154–157, 159
- Subtrack mode, mobile target tracking, 190
- Summarization, 271–272
- Suppression, distributed mobile target tracking, 183–184
- Surveillance
 - military operations, 283, 294
 - mobile target tracking, 189, 191
 - using wireless sensor network, 197, 224
- Sweep coverage, 224
- Switched networks, 32
- Sybil attacks, 288, 299
- Synchronous orthogonal CDMA system, 95
- Synthetic mobility models, 18
- Sysadmins, 25
- Syslog
 - campus WLAN studies, 17, 19
 - characterized, 24–25
 - WLAN measurement studies, 6–10, 22
- TAG, 271
- Tampering, 287
- Target tracking, sensor networks, 142.
 - See also* Mobile target tracking (MTT)
- Tcpdriv, 33
- Tcpdump, 12–13, 18–19, 33
- TEA, 290
- TEEN, 299
- Telnet, 17–18, 325
- TESLA, 291, 302
- Third-generation cellular systems, 93
- Throughput capacity, field gathering wireless sensor networks, 211
- Time-division multiple access (TDMA), 95, 215
- Timescale, MANETs, 84
- Time synchronization, 184, 302
- TinyDB, 264
- TinyOS, 263, 299
- Topology control
 - algorithms, MANETs, 82–83
 - wireless sensor networks, 222
- TORA, multihop wireless networks, 125
- Total coverage, wireless sensor networks, 227

- Total transmission energy, 2
- Trace/tracing
 - collection, 32–33
 - data, 40–42
 - gathering, campus WLAN usage studies, 30, 33
 - traffic, 33
- Tracking stage, mobile target tracking, 189
- Track maintenance, mobile target tracking (MTT), 184–185
- Traffic
 - authentication, 296
 - campus WLAN usage studies, 32
 - flow, wireless sensor networks, 252
 - patterns, 17
 - permutation attack, 369–370
 - specification (TSPEC), 54
 - streams (Tss)
 - QoS provisioning, 54
 - rate of, 48
- Transistor–transistor logic (TTL), 325
- Transmission control protocol (TCP)
 - multihop wireless networks
 - energy costs, 112–114
 - reliable packet transmissions, 122–123
 - QoS provisioning
 - access, EDCA default vs. PIFs, 66, 70
 - flow, single VoIP queue, 58–63
 - packet headers, implications of, 30, 56–57
 - traffic, campus wireless networks, 40
 - wireless sensor networks, 325, 328
- Transmission energy, multihop wireless networks, 109–110
- Transmission floor, 75
- Transmission mode, MANETs, 75–76
- Transmission opportunity (TXOP), 51
- Transmission power
 - control, *see* Transmission power control (TPC)
 - field gathering wireless sensor network, 210–211, 213, 215
 - levels of, 2
- Transmission power control (TPC)
 - CDMA-based ad hoc networks, 95–96, 100
 - implications of, 2, 82
 - MANETs
 - data packets, 77–78
 - directional antennas, 93–95
 - implications of, 73
 - interference-aware MAC design/protocol, 84–91
 - PARP/SIMPLE approach, 81–82, 99
 - power-aware routing protocols (PARPs), 78–81
 - SIMPLE approach, 78–80
 - topology control algorithms, 82–83
 - mobility issues, 90
 - transmission rate control, 92–93
- Transmission queue, 48
- Transmission range
 - critical, 229
 - field gathering wireless sensor networks, 210–211, 213, 215
 - MANETs, 76–77
 - wireless sensor network, 201
- Transmission rate control, MANETs, 92–93
- Transmission schedule, field gathering wireless sensor networks, 215
- Transport capacity, field gathering wireless sensor networks, 210, 212
- Tree management, 185–187
- Tribal Nations, 382
- Trust routing for location aware sensor networks (TRANS), 299
- Turnaround time, 90
- Two-channel architecture, 85–86
- Two-phase clustering, 253
- Type loss, 14–15
- UDP
 - multihop wireless networks, 118, 121, 135
 - packets, 30
 - traffic, campus wireless networks, 40
 - transport, 10, 55
- Ultra-low-power RF radios, 270
- Unauthorized traversal (UT) algorithm, 233–234
- Uncertainty-aware sensor deployment algorithm (UADA), 246, 248
- Unicast packets, wireless networks, 127
- Uninterrupted power supply (UPS), 13
- U.S. Defense Advanced Research Projects Agency (DARPA), 406
- U.S. National Science Foundation, 339
- Universal data compression, 348

- Universal description, discovery, and integration (UDDI), 329
- University of California San Diego, campus WLAN studies, 18
- University of Maryland, wireless-side measurement studies, 21–22
- University of North Carolina at Chapel Hill, campus WLAN usage studies, 31
- University of Saskatchewan, campus WLAN usage, 18, 29–30
- Unix timestamp, 9
- Unstructured networks, storage management, 274
- URLs, 17
- Usage peaks, campus WLAN studies, 17
- User behavior, 17

- Variable-power transmission, multihop wireless networks, 127–128, 136
- Vector-based algorithm (VEC), 242–243, 248
- Virtual force algorithm (VFA), 240–241, 247
- Virtual MAC (VMAC), 48
- Virtual polar coordinate space (VPCS), 277
- Virtual source (VS) algorithm, 48
- Viruses, 25
- Vision Media Technologies, Inc., 382
- Visual surveillance, 259
- VLANs, 25
- Voice codecs, 55
- Voice over Internet Protocol (VoIP)
 - for admission control
 - characterized, 55, 70
 - 802.11b capacity for, 56, 58
 - campus WLAN usage studies, 19, 32
 - characterized, 1, 393
 - quality of service, 45–46, 50
- Voltage controlled oscillators (VCOs), 92
- VOR algorithm, 242–243, 248
- Voronoi-based algorithm (VOR) 242–243, 248
- Voronoi diagrams, 233, 235–236, 242, 252
- Voronoi neighbors, 235
- Voronoi polygons, 242–243

- Waiting mode, mobile target tracking, 190–191
- Wakeup
 - rate, 251
 - signals, 97
 - state, 251
- WAKEUP message, wireless sensor network, 193
- Warehouses, inventory management, 197
- Weather
 - conditions, impact of, 259, 341
 - monitoring, 383
- Web Service Description Language (WSDL), 330
- Web services, 319–320
- Weighted moving average, 128–129
- Weighting, cooperative mobile target tracking, 179–180
- WiFi (wireless fidelity), 31, 382, 404–405
- Wildlife tracking sensor network, 259
- Windows Update, 13
- WINMEC, 309, 332
- WinRFID
 - architecture of, 323, 330
 - functions of, 309, 313, 324, 328–332
 - rule engine, 330
 - runtime plugins, 330–331
 - services
 - reader web service, 329–330
 - reader windows services, 328
 - remote object based service, 328
- Wireless ad hoc networks, 2
- Wireless clients, misconfigured, 25
- Wireless-enabled devices, 105
- Wireless Internet service providers, 382
- Wireless intrusion protection system, 14
- Wireless inventory tracking devices, 32
- Wireless LANs (WLANS)
 - 802.11 infrastructure network, 6
 - measurement studies of traffic, 1, 5–24
 - popularity of, 1
- Wireless measurement checklist, 24–25
- Wireless sensor networks, multipath routing, 299
- Wireless sniffing, WLAN measurement studies, 14–15, 22, 24
- Wireless transceiver, 286
- Wireless usage studies
 - benefits of, 5
 - campus WLANs, 16–20
 - data collection, 5–6
 - long-term, 16
 - manually obtained data, 16

- Wireless usage studies (*Continued*)
 - measurement tools
 - authentication logs, 11–12
 - client-side tools, 15–16
 - network sniffing, 12–13
 - SNMP, 10–11, 17
 - syslog, 6–10
 - wireless sniffing, 14–15
 - methodologies, 22–24
 - nonacademic WLANs, 20–21
 - wireless measurement checklist, 24–25
 - wireless-side measurement studies,
 - 21–22
- Wireline network, campus WLAN usage studies, 31–32
- Working node, wireless sensor network, 251
- World Wide Web (WWW)
 - browsing, 17, 21
 - traffic, 19
- Wormholes, 299
- Worms, 25
- X10, smart environment features, 340, 343, 352
- ZoomAir, 22