Implications of unlicensed mobile access (UMA) for GSM security p. 3
Computational, memory, and bandwidth efficient distillation codes to mitigate DoS in multicast p. 13
Spread-identity mechanisms for DoS resilience and security p. 23
On the security of distributed position services p. 35
Picking virtual pockets using relay attacks on contactless smartcard systems p. 47
A lightweight RFID protocol to protect against traceability and cloning attacks p. 59
An RFID distance bounding protocol p. 67
Security and privacy issues in e-passports p. 74
DICAS : detection, diagnosis, and isolation of control attacks in sensor networks p. 89

Securing topology maintenance protocols for sensor networks : attacks and countermeasures p. 101
Countermeasures against traffic analysis attacks in wireless sensor networks p. 113
Improving cross-domain authentication over wireless local area networks p. 127
Reducing reauthentication delay in wireless networks p. 139
Providing distributed certificate authority service in mobile ad hoc networks p. 149
On improving the performance of role-based cascaded delegation in ubiquitous computing p. 157
A privacy preserving reputation system for mobile information dissemination networks p. 171
A privacy service for context-aware mobile computing p. 182
Protecting location privacy through path confusion p. 194
A solution for wireless privacy and payments based on e-cash p. 206
Short paper : a signal fingerprinting paradigm for general physical layer and sensor network security and assurance p. 219
Short paper : location privacy with IP mobility p. 222
Short paper : fellowship in mobile ad hoc networks p. 225
Short paper : a secure interworking scheme for UMTS-WLAN p. 228
Short paper : bufSTAT - a tool for early detection and classification of buffer overflow attacks p. 231
Short paper : towards a location-aware role-based access control model p. 234
Short paper : tri-party TLS adaptation for trust delegation in home networks p. 237
Short paper : PATRIOT - a policy-based, multi-level security protocol for safekeeping audit logs on wireless devices p. 240
Short paper : harnessing emergent ubiquitous computing properties to prevent malicious code propagation p. 243
A level key infrastructure for secure and efficient group communication in wireless sensor networks p. 249
A modified secure remote password (SRP) protocol for key initialization and exchange in Bluetooth systems p. 261
An efficient key management algorithm for hierarchical group communication p. 270
A deterministic pairwise key pre-distribution scheme for mobile sensor networks p. 277
A practical study of transitory master key establishment for wireless sensor networks p. 289
Applying emergence to the design of routing protocols for the security of wireless ad hoc networks

SPINAT: integrating IPsec into overlay routing

On the survivability of routing protocols in ad hoc wireless networks

An extensible environment for evaluating secure MANET

Soft-timeout distributed key generation for digital signature based on elliptic curve D-log for low-power devices

A uniform framework for cryptanalysis of the Bluetooth $E_0$ cipher

MOTET: mobile transactions using electronic tickets

Exploiting hierarchical identity-based encryption for access control to pervasive computing information

Short paper: GKE: efficient group-based key establishment for large sensor networks

Short paper: practically unbounded one-way chains for authentication with backward secrecy

Short paper: limitations of key escrow in identity-based schemes in ad hoc networks

Short paper: enhanced 1-D chaotic key-based algorithm for image encryption

Short paper: schemes for enhancing the denial-of-service tolerance of SRTP

Short paper: thor - the hybrid online repository

Short paper: random IDs for preserving location privacy

Short paper: a distributed cross-layer intrusion detection system for ad hoc networks

Short paper: dynamic risk mitigation for ‘self-defending’ network security

Table of Contents provided by Blackwell's Book Services and R.R. Bowker. Used with permission.